FortiClient EMS - Admin Guide

Version 1.2.3

FORTINET DOCUMENT LIBRARY
http://docs.fortinet.com

FORTINET VIDEO GUIDE
http://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTIGATE COOKBOOK
http://cookbook.fortinet.com

FORTINET TRAINING SERVICES
http://www.fortinet.com/training

FORTIGUARD CENTER
http://www.fortiguard.com

END USER LICENSE AGREEMENT
http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

December 13, 2017
FortiClient EMS 1.2.3 Admin Guide
04-123-408881-20171213

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-12-13	Initial release.

Introduction

FortiClient Enterprise Management Server (FortiClient EMS) is a security management solution that enables scalable and centralized management of multiple endpoints (computers). FortiClient EMS provides efficient and effective administration of endpoints running FortiClient. It provides visibility across the network to securely share information and assign security profiles to endpoints. It is designed to maximize operational efficiency and includes automated capabilities for device management and troubleshooting.

FortiClient EMS is designed to meet the needs of small to large enterprises that deploy FortiClient on endpoints. Benefits of deploying FortiClient EMS include:

- Remotely deploying FortiClient software to Windows PCs
- Updating profiles for endpoint users regardless of access location, such as administering antivirus, web filtering, VPN, and signature updates
- Administering FortiClient endpoint connections, such as accepting, disconnecting, and blocking connections
- Managing endpoints, such as status, system, and signature information
- Identifying outdated versions of FortiClient software

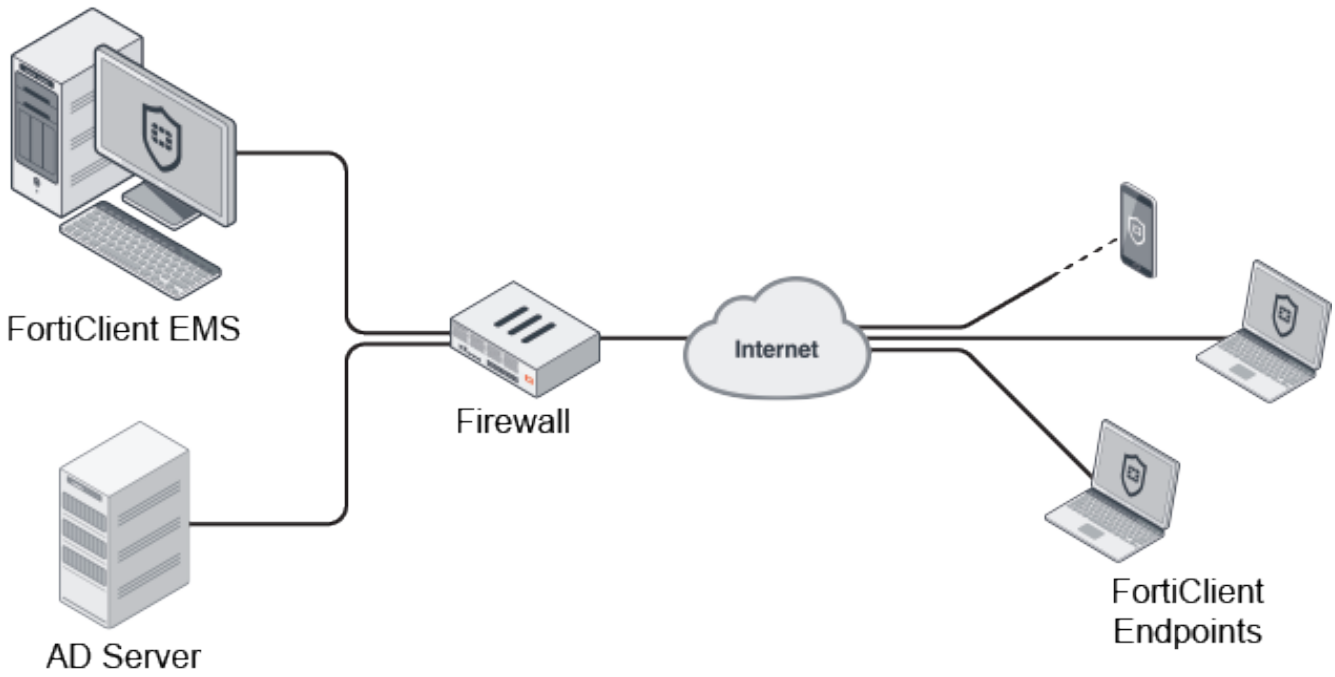
You can manage endpoint security for Windows and Mac OS X platforms using a unified organizational security policy. An organizational security policy provides a full, understandable view of the security policies defined in the organization. You can see all policy rules, assignments, and exceptions in a single unified view.

FortiClient EMS components

FortiClient EMS provides the infrastructure to install and manage FortiClient software on endpoints. FortiClient protects endpoints from viruses, threats, and risks.

The following table lists FortiClient EMS components.

Component	Description
FortiClient EMS	Manages FortiClient on endpoints that connect to your network. It includes the following software: • Console software that manages security profiles and FortiClient on endpoints • Server software that provides secure communication to and from endpoints and the console
Database	Stores security profiles and events. The SQL database is installed as part of the FortiClient EMS installation.
FortiClient	Helps enforce security and protection on endpoints. It runs on servers, desktops, and portable computers you want to secure. See the *FortiClient Administration Guide* on docs.fortinet.com/forticlient/admin-guides for information.



FortiClient EMS allows you to:

- Establish and enforce security profiles
- Manage deployment, configuration, and updates
- Obtain a consolidated view of multiple security components across all endpoints in your network
- Perform integrated installation of security components and set profiles

An informative video introducing you to FortiClient EMS is available in the Fortinet Video Library.

FortiClient EMS and Fortinet Endpoint Security Management

FortiClient EMS is part of the Fortinet Endpoint Security Management suite, which ensures comprehensive policy administration and enforcement for an enterprise network.

Documentation

You can access FortiClient EMS documentation from the following link: docs.fortinet.com/ems/admin-guides

The FortiClient EMS documentation set includes the following:

- *FortiClient EMS 1.2.3 Release Notes*

  This document describes new features and enhancements in FortiClient EMS for the release and lists any known issues and limitations. This document also defines supported platforms and minimum system requirements.
- *FortiClient EMS 1.2.3 QuickStart Guide*

  This document describes how to install and begin working with the FortiClient EMS system. It provides instructions on installation and deployment, and includes a high-level task flow for using the FortiClient EMS system.
- *FortiClient EMS 1.2.3 Administration Guide*

  This document describes how to set up FortiClient EMS and use it to manage FortiClient endpoints. It includes information on how to configure multiple endpoints, configure and manage profiles for the endpoints, and view and monitor FortiClient endpoints.
- *FortiClient EMS Upgrade Paths*

  This document provides upgrade path information for different versions of FortiClient EMS.

What's New

The following is a list of new features and enhancements in FortiClient EMS 1.2.

FortiClient EMS 1.2.3

FortiClient EMS 1.2.3 does not contain new features or enhancements.

FortiClient EMS 1.2.2

Redesigned navigation menu

The left navigation menu has been redesigned to provide easier access to the content pane on the right. The top menu has also been merged into the left navigation menu.

New Dashboard

The new Dashboard includes new chart designs and easier access to information and alerts. Administrators can customize the dashboard by moving widgets around. See Dashboard on page 41.

Sign custom FortiClient installer

You can now sign FortiClient installers created in FortiClient EMS with your own certificate. See Configuring Server settings on page 111.

FortiSandbox authorization of FortiClient

FortiClient EMS administrators can configure a FortiSandbox IP address in an endpoint profile. After the configuration is saved, FortiClient EMS attempts to submit an authorization request to, and check if it is authorized with, the configured FortiSandbox. If the FortiSandbox administrator authorizes FortiClient EMS, the authorization status displays on the FortiClient EMS GUI. Subsequently, all FortiClient endpoints managed by FortiClient EMS are considered authorized by the same FortiSandbox.

This feature requires FortiSandbox 2.5.0 and FortiClient 5.6.1.

FortiClient EMS 1.2.1

FortiClient EMS 1.2.1 does not contain new features or enhancements.

FortiClient EMS 1.2.0

Customize FortiClient installer

FortiClient EMS can create a FortiClient installer with any of the following components:

- SFA: The Security Fabric Agent provides endpoint telemetry, host vulnerability scanning, and remediation. This component is always selected and cannot be deselected.
- SAA: Secure Access Architecture Components include SSL VPN and IPSec VPN features. This component is selected by default.
- APT: Advanced Persistent Threat Components provide integration with FortiSandbox detection.
- ASF: Additional Security Features include AntiVirus, Web Filtering, Application Firewall, and Single Sign-On mobility agent.

See Software Management on page 104.

FortiClient for Mac OS X Vulnerability Scan support

FortiClient for Mac OS X now supports Vulnerability Scan and auto-patching features. See Endpoint Profiles on page 64.

One-time pull of an existing FortiClient profile from FortiGate

FortiClient EMS now supports a one-time pull of an existing FortiClient profile from FortiGate. The EMS admin can pull an existing FortiClient profile from a FortiGate and modify it before deploying to endpoints. See Importing FortiGate profiles on page 67.

Pre-login banner

The pre-login banner can be used to display a message on the login page for FortiClient EMS before the user logs in. Users must accept the banner message before they can log in. See Configuring the login banner on page 115.

Deployment improvements

FortiClient EMS has improved the installer deployment functionality so more realtime deployment information is visible on FortiClient EMS. The deployment technique has been enhanced so it is more reliable and provides a better user experience. See Viewing endpoints on page 51.

Redesigned Endpoints pane

The *Endpoints* pane has been redesigned to be more user-friendly. You can clearly see the endpoint installer deployment, profile synchronization, FortiClient Telemetry connection, and compliance status. The device information is also better organized for easier access. See Viewing the Endpoints content pane on page 51.

Get Started

This section provides an overview of how to perform the following tasks after you install FortiClient EMS:

Deploying FortiClient software to endpoints

Following is an overview of how to add endpoints to FortiClient EMS and configure FortiClient EMS to deploy FortiClient to endpoints.

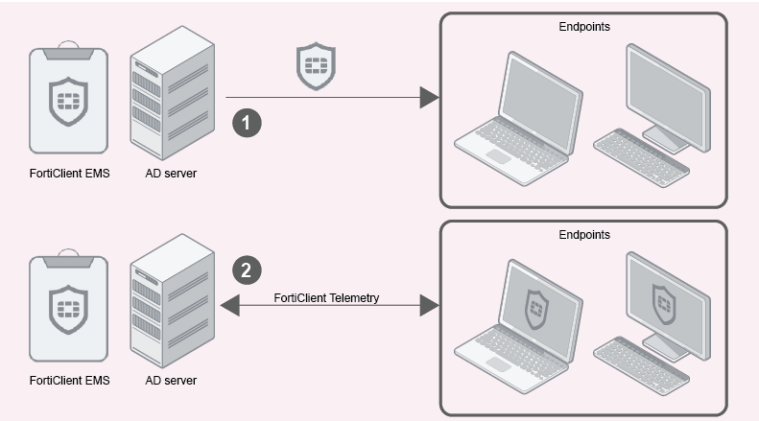
You can deploy FortiClient to endpoints using AD servers and workgroups. There are differences between using AD servers and workgroups.

When using an AD server, you can deploy an initial installation of FortiClient (Windows) to endpoints, but you cannot deploy an initial installation of FortiClient (Mac OS X). After FortiClient for Windows or Mac OS X is installed on endpoints and endpoints are connected to FortiClient EMS, you can deploy upgrades, uninstallations, and replacements of both FortiClient for Windows and Mac OS X using AD servers.

When using workgroups, you cannot deploy an initial installation of FortiClient to endpoints. However, after FortiClient is installed on endpoints and endpoints are connected to FortiClient EMS, you can use workgroups to uninstall and update FortiClient on endpoints.

The image below shows a deployment of FortiClient using FortiClient EMS with an AD server:

1. Deploy FortiClient from FortiClient EMS using an AD server to the desired endpoints.
2. The endpoints now have FortiClient installed and FortiClient Telemetry is connected to FortiClient EMS.

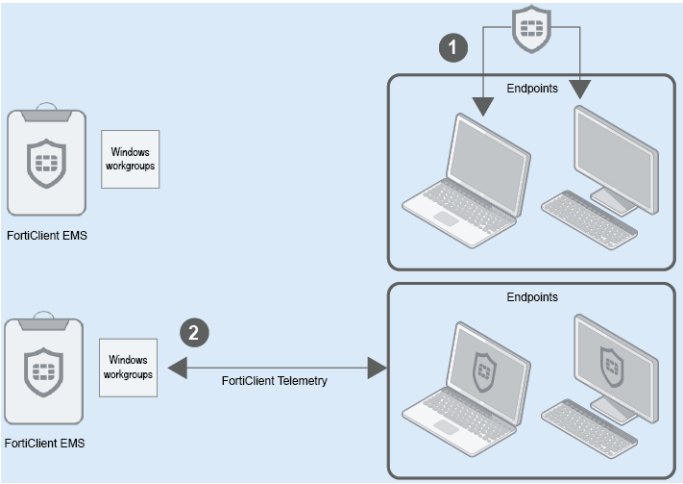


The image below shows a deployment of FortiClient (Windows) using FortiClient EMS with Windows workgroups:

1. Workgroups cannot be used with FortiClient EMS to initially install FortiClient on endpoints. FortiClient must be installed directly on endpoints. Endpoint users can access *Software Management* in FortiClient EMS to download

and install FortiClient on endpoints. See Viewing installers in Software Management on page 107.

2. The endpoints now have FortiClient installed and FortiClient Telemetry is connected to FortiClient EMS.



To deploy FortiClient software to endpoints:

1. Add endpoint with an AD server or Windows workgroups. See Adding endpoints on page 49.

   Endpoints added using an AD service are displayed on the *Endpoints* > *Domains* pane, and endpoints added using Windows workgroups are displayed on the *Endpoints* > *Workgroups* pane. You can install, upgrade, and uninstall FortiClient on endpoints using an AD server without connecting FortiClient to FortiClient EMS as long as the username and password are correct on the profile's *Deployment* tab in FortiClient EMS. Note workgroups can only be used to upgrade or uninstall FortiClient if it is already installed on the endpoints and connected to FortiClient EMS; workgroups cannot be used for initial installations of FortiClient. When using workgroups, the credentials on the *Deployment* tab in FortiClient EMS are not taken into account.
2. Add FortiClient installers to FortiClient EMS, and specify which FortiClient features each installer will install on endpoints. See Adding FortiClient installers on page 105.
3. Create a profile to select the FortiClient installer and include configuration information for FortiClient software on endpoints. See Creating profiles to deploy FortiClient on page 65.
4. Prepare domains and workgroups for deployment. See Preparing the AD server for deployment on page 94.
5. Assign profiles to domains and workgroups to deploy FortiClient on endpoints. See Assigning profiles to endpoints on page 70.

   See Deploying FortiClient on endpoints on page 96.

   After the profile is assigned to endpoints, its changes are pushed to endpoints. FortiClient is installed on endpoints, and FortiClient connects Telemetry to FortiClient EMS.
6. Monitor the installation process using the *Endpoints* content pane. See Viewing the Endpoints content pane on page 51.

Pushing configuration information to FortiClient

After the endpoints' FortiClient connects FortiClient Telemetry to FortiClient EMS, the endpoints are managed, and you can use FortiClient EMS to push configuration information to FortiClient software on endpoints.

To push configuration information to FortiClient:

1. Edit an existing profile or create a new profile to configure FortiClient software on endpoints. See Creating profiles to configure FortiClient on page 64.
2. Assign profiles to domains and workgroups to deploy FortiClient on endpoints. See Assigning profiles to endpoints on page 70.

   After the profile is assigned to endpoints, its changes are pushed to endpoints with the next Telemetry communication.
3. Monitor the update using the *Endpoints* content pane. See Viewing the Endpoints content pane on page 51.

Relationship between FortiClient EMS, FortiGate, and FortiClient

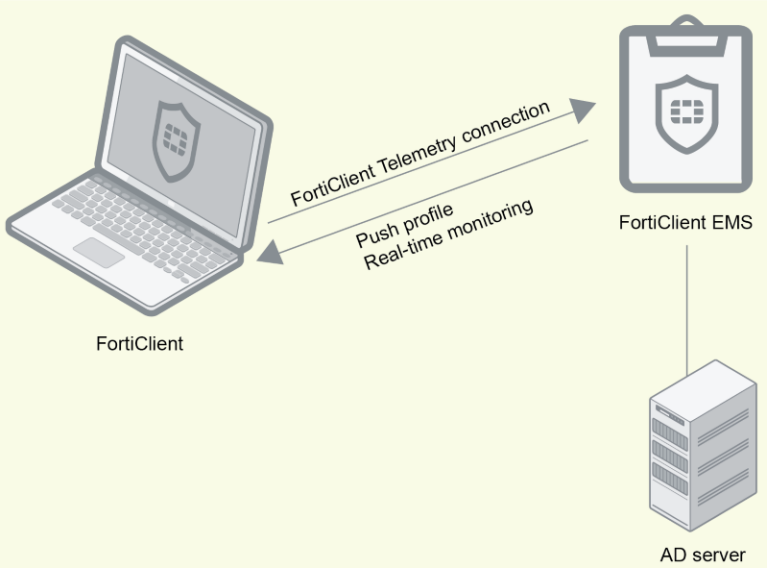
FortiClient EMS can be used in standalone mode or integrated with FortiGate. The following section illustrates the topology for each configuration and the GUI differences between the scenarios. The following table clarifies the terminology used:

Term	Definition
Primary Telemetry connection	The following are primary Telemetry connections: • Connection between FortiClient and FortiOS when FortiClient is used with FortiGate. See FortiClient EMS integrated with FortiGate on page 18. • Connection between FortiClient and EMS when FortiClient is used without FortiGate and the user manually connects FortiClient Telemetry to EMS.
Secondary Telemetry connection	The following are secondary Telemetry connections: • Connection between FortiClient and EMS when FortiClient is used with FortiGate and EMS. See FortiClient EMS integrated with FortiGate on page 18. • Connection between FortiClient and EMS when FortiClient is used without FortiGate and FortiClient is deployed using an installer created in EMS or gateway IP lists are used to connect FortiClient and EMS.

For details, see the *FortiClient Compliance Guide*.

Standalone FortiClient EMS

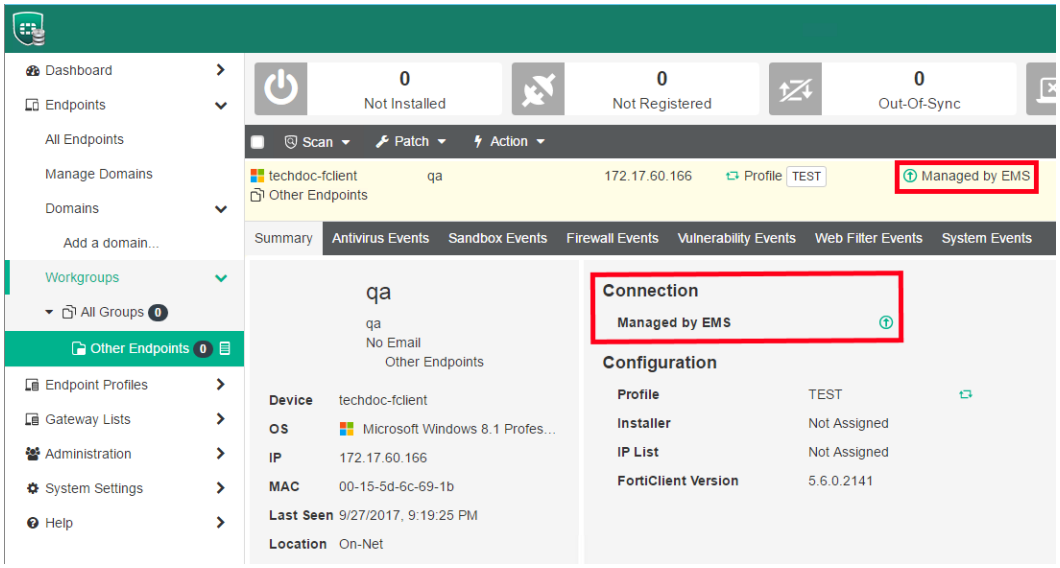
The diagram below shows the topology when using FortiClient EMS in standalone mode.

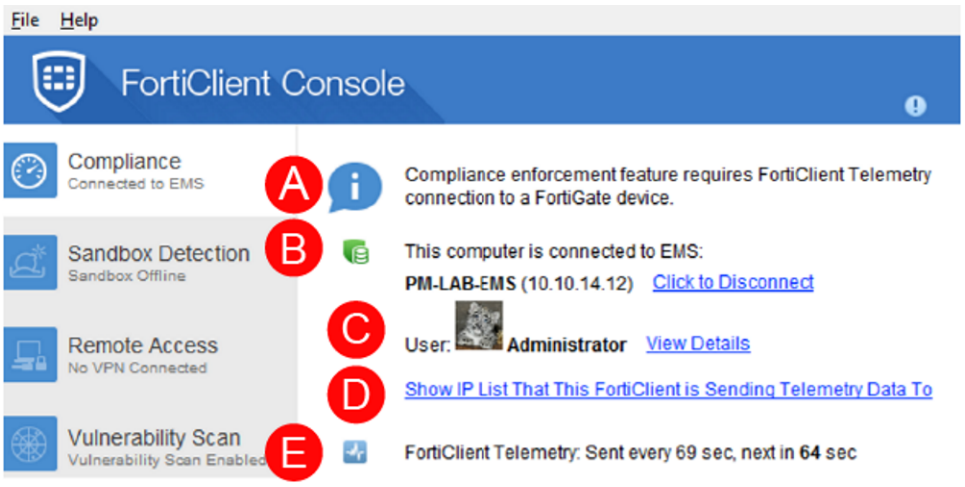


In this scenario, FortiClient EMS provides FortiClient endpoint provisioning. FortiClient endpoints connect FortiClient Telemetry to FortiClient EMS to receive configuration information from FortiClient EMS. This scenario does not support compliance.

If the user manually enters the EMS server's IP address in FortiClient Console to establish the Telemetry connection, this connection is a primary Telemetry connection. If FortiClient is deployed using an installer created in EMS or a gateway IP list is used to connect FortiClient and EMS, this connection is a secondary Telemetry connection. For details on how the secondary Telemetry connection differs from the primary Telemetry connection, see the *FortiClient Compliance Guide*.

When viewing the endpoint in the FortiClient EMS GUI, the endpoint's connection is shown as *Managed by EMS*.

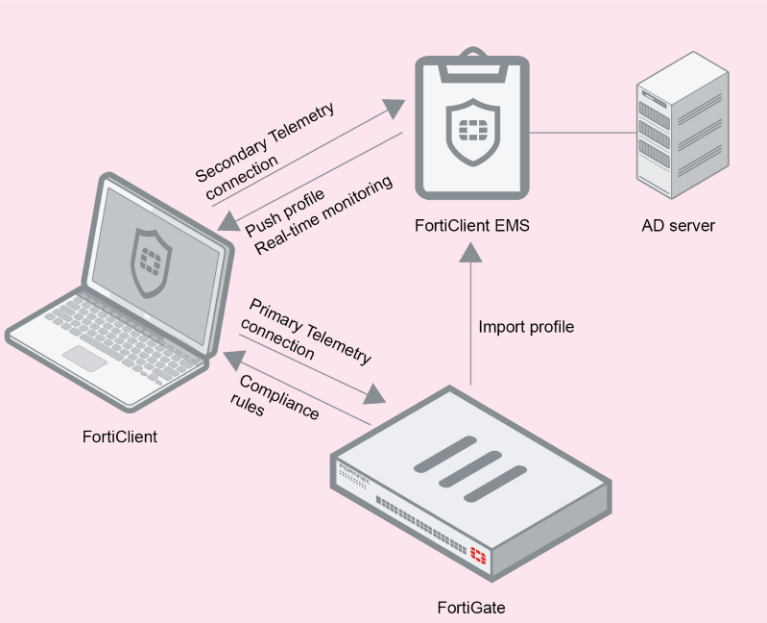




Label	Description
A	This shows there is currently no compliance enforcement because FortiClient is not connected to a FortiGate.
B	View the name and IP address of the EMS to which FortiClient Telemetry is connected. This means FortiClient EMS can push profiles to FortiClient. FortiClient EMS is providing endpoint provisioning to FortiClient.
C	View details about the user logged into the endpoint.
D	Click the *Show IP List That This FortiClient is Sending Telemetry Data To* link to view the gateway IP list being used for FortiClient Telemetry connection. Administrators create the Telemetry gateway list. Endpoint users cannot change the list.
E	View how often FortiClient Telemetry communicates with FortiClient EMS and when the next communication will occur. FortiClient Telemetry communicates information between FortiClient and EMS.

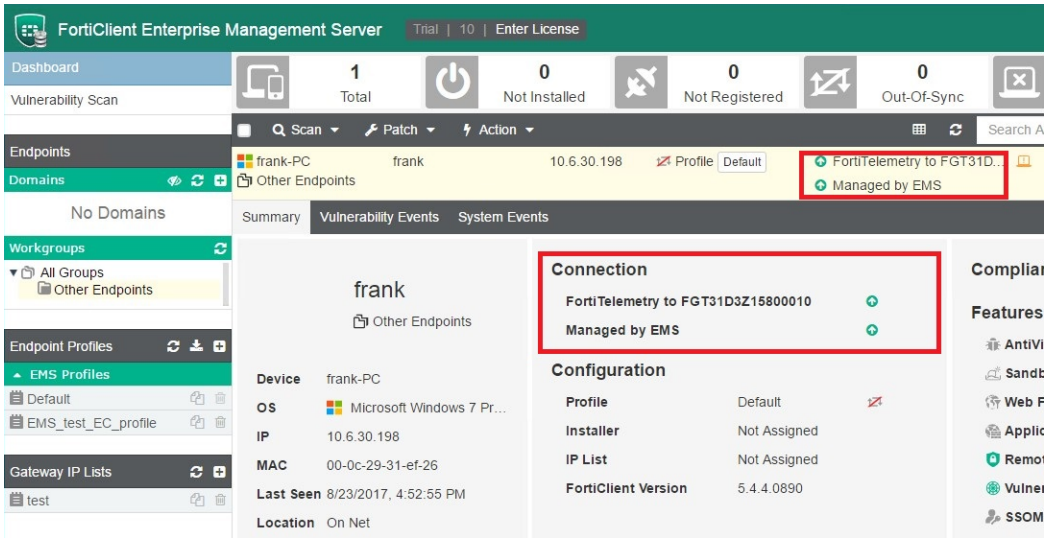
FortiClient EMS integrated with FortiGate

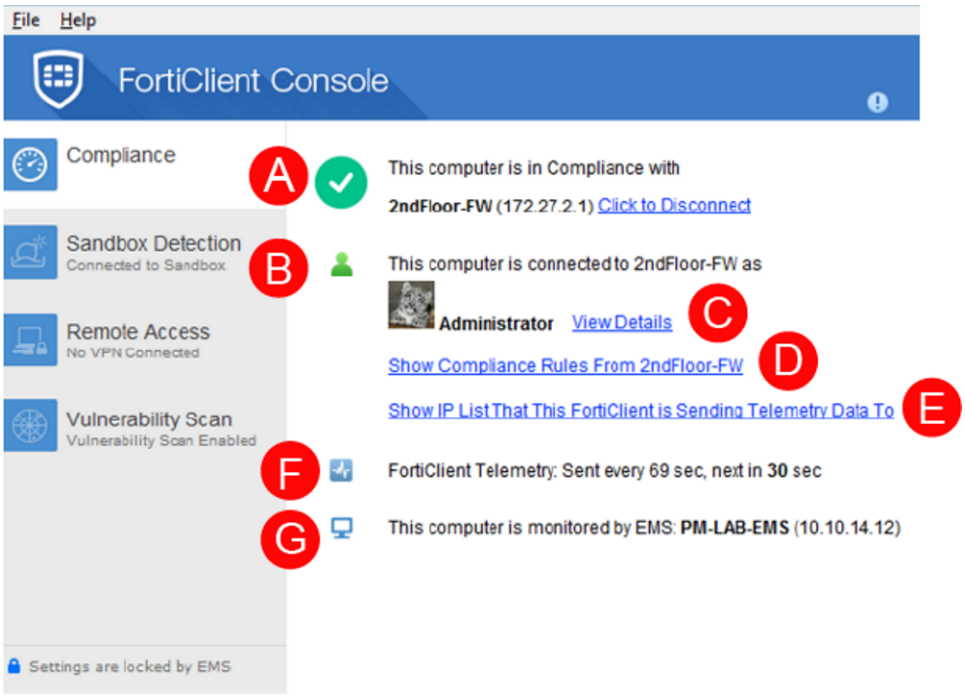
The diagram below shows the topology when using FortiClient EMS integrated with FortiGate.



In this scenario, FortiClient EMS provides FortiClient endpoint provisioning, while the FortiGate provides compliance rules to the endpoint. FortiClient endpoints connect FortiClient Telemetry to FortiClient EMS to receive configuration information from FortiClient EMS and receive compliance rules from the FortiGate. Profiles can also be imported from the FortiGate to FortiClient EMS, then pushed to the endpoints.

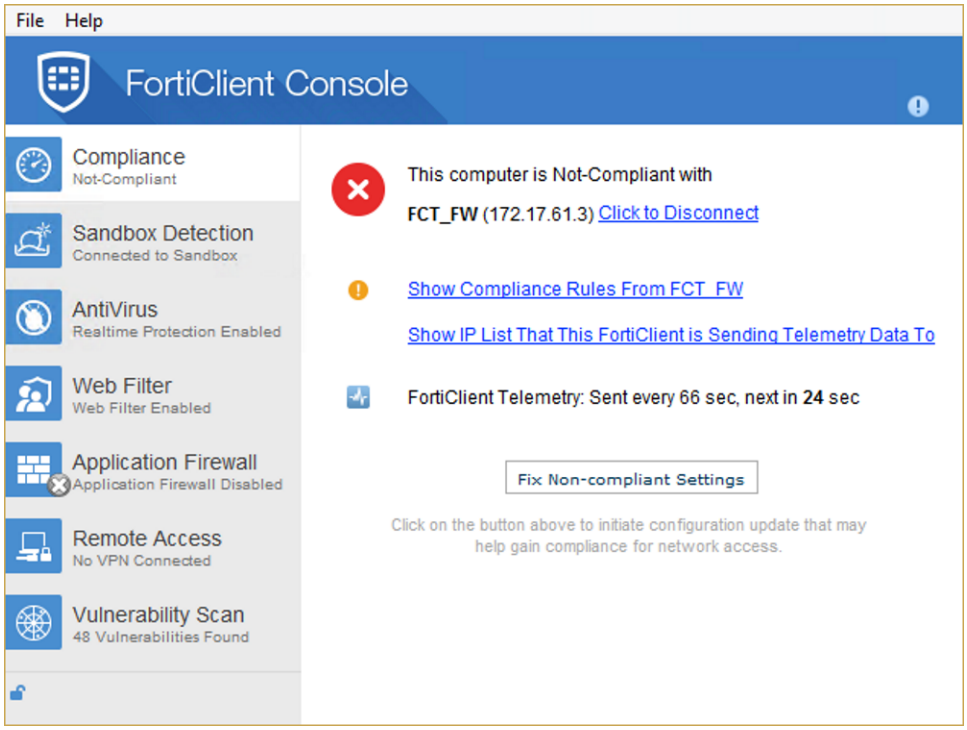
When viewing the endpoint in the FortiClient EMS GUI, the endpoint's connection is shown as *FortiTelemetry to FGT<number>* and *Managed by EMS*.



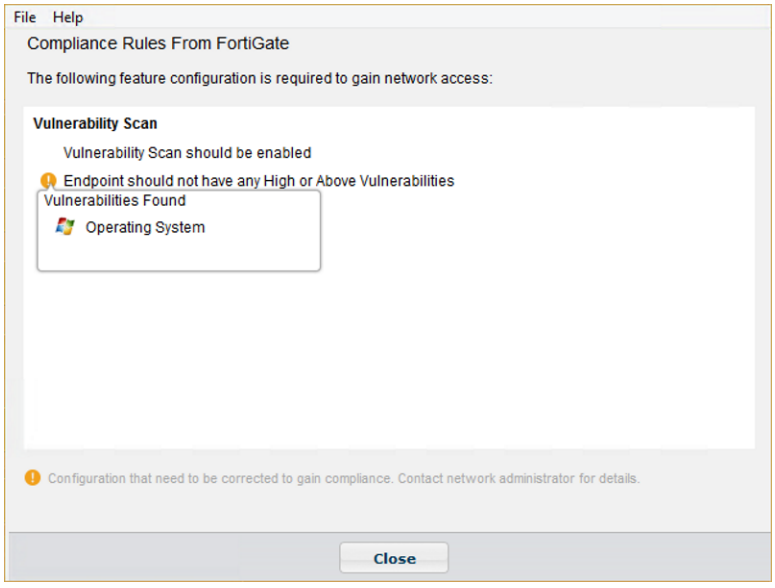


Label	Description
A	This shows the endpoint is connected to the specified FortiGate and is compliant to security policy rules defined under FortiClient profiles on that FortiGate.
B	This shows the endpoint is connected to and receiving compliance rules from the specified FortiGate.
C	View details about the logged in user.
D	When FortiClient Telemetry is connected to FortiGate, you can view the compliance rules from FortiGate. The compliance rules communicate the configuration required for FortiClient Console and the endpoint to remain compliant. When the endpoint has a non-compliant status, an exclamation mark indicates which compliance rules are not met. See below for an example of the FortiClient Console GUI when the endpoint is not compliant.
E	View the Telemetry gateway list or the remembered FortiGate list. Administrators create the Telemetry gateway list. Endpoint users cannot change the list. Endpoint users create the remembered FortiGate list. It is the list of remembered gateway IP addresses for FortiGate and EMS. When FortiClient Telemetry is connected for the first time, you can instruct FortiClient to remember the gateway IP address for FortiGate or EMS. The gateway IP lists are used to automatically connect FortiClient Telemetry to FortiGate or EMS.
F	View how often FortiClient Telemetry communicates with FortiGate and FortiClient EMS and when the next communication will occur. FortiClient Telemetry communicates information between FortiClient and FortiGate, sending status information to FortiGate and receiving network-access rules from FortiGate. Notification information is also sent to EMS. EMS also sends endpoint profiles of configuration information to FortiClient.
G	View the FortiClient EMS server's name. This indicates FortiClient EMS is managing and provisioning configuration to the endpoint.

The below shows an example of the FortiClient Console when the endpoint is not compliant with FortiGate compliance rules and may be blocked from accessing the network.

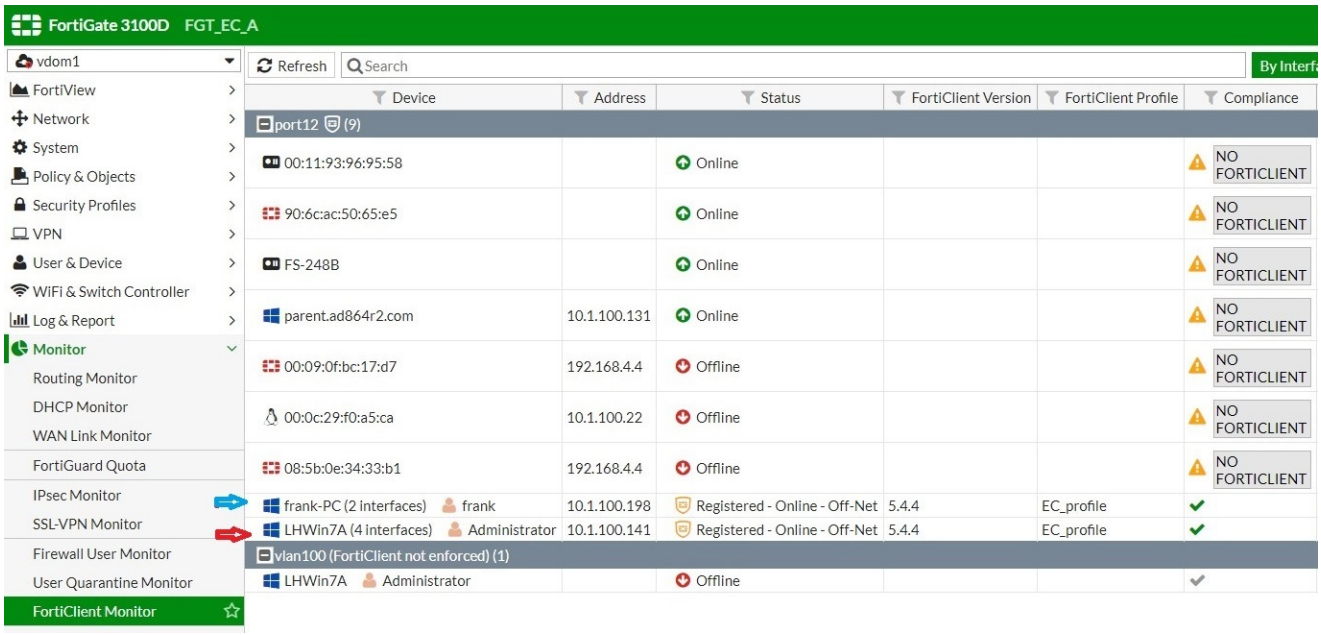


You have some time to fix the non-compliant issues before FortiGate blocks network access. When an endpoint has a non-compliant (blocked) status, you can view the compliance rules from FortiGate and identify which ones are causing the non-compliant status by clicking *Show Compliance Rules From <FortiGate>*.



You can fix non-compliant settings by clicking *Fix Non-Compliant Settings*. For details, see the *FortiClient Administration Guide*.

The image below shows the FortiOS GUI. In this situation, frank-PC and LHWin7A represent two endpoints connected to the FortiGate. frank-PC is also managed by FortiClient EMS. There is no flag to identify between the scenarios.



Using EMS integrated with FortiGate

You can integrate FortiGate with FortiClient EMS. When used together, FortiGate is used for endpoint control and network access compliance (NAC), and FortiClient EMS is used to deploy and manage FortiClient software on endpoints.

When FortiGate is configured for NAC, you can use FortiOS to create a FortiClient profile that defines compliance rules and non-compliance action. The compliance rules define what configuration FortiClient software and the endpoint must have for the endpoint to maintain access to the network through FortiGate. The non-compliance action can be *block* or *warn* and defines what action FortiGate takes when endpoints fail to comply with the compliance rules. When the non-compliance action is *block*, FortiGate blocks endpoints from accessing the network when they fail to comply with the compliance rules. When the non-compliance action is *warn*, FortiGate warns the endpoint about non-compliance but allows network access after the endpoint user acknowledges the warning.

Although the compliance rules define what configuration FortiClient software and the endpoint must have, the FortiClient profile from FortiGate does not include any configuration information. The endpoint user or administrator is responsible for configuring FortiClient Console to adhere to the compliance rules. An administrator can use FortiClient EMS to configure FortiClient Console.

After you create a FortiClient profile using FortiOS, you can import the profile into FortiClient EMS and edit the profile to add a FortiClient installer and specify configuration information for FortiClient software. Then you can use FortiClient EMS to deploy the updated profile containing compliance rules and configuration information to endpoints.

To use EMS integrated with FortiGate:

1. Using FortiGate running FortiOS 5.6, create a FortiClient profile to define the compliance rules.
2. Using FortiClient EMS, import the FortiClient profile. See Importing FortiGate profiles on page 67.

3. Review the compliance rules.
4. Edit the imported profile to add configuration information that supports the compliance rules, and save the profile. You can add a FortiClient installer if needed.
5. Create a gateway IP list that includes the gateway IP address or fully qualified domain name (FQDN) for the FortiGate. See Creating gateway IP lists on page 91.

   Each gateway IP list includes a list of one or more IP addresses or fully qualified domain names (FQDN) that FortiClient can use when registering to EMS or FortiGate.
6. Assign the gateway IP list to domains or workgroups as needed. See Assigning gateway IP lists to endpoints on page 93.

   FortiClient software uses the IP addresses in the gateway IP list to connect FortiClient Telemetry to EMS and/or FortiGate.
7. Assign the profile to domains or workgroups as needed. See Assigning profiles to endpoints on page 70.

   After the profile is assigned to endpoints, the compliance rules and settings are pushed to endpoints with the next Telemetry communication.
8. Use FortiClient EMS to monitor and manage endpoints. See Viewing the Endpoints content pane on page 51.
9. Use FortiClient EMS to update the profile as needed.

Installation Preparation

This section helps you prepare to install FortiClient EMS. Before installing FortiClient EMS, be aware of the following information.

Before installing FortiClient EMS, it is recommended you read the *FortiClient EMS Release Notes* available on http://docs.fortinet.com/ems/release-information to become familiar with relevant software components and other important information about the product.

Licenses

This section describes licensing options available for FortiClient EMS. It provides information about the number of supported FortiClient endpoints for each type of license to help determine which license best suits your needs.

FortiClient EMS

FortiClient EMS supports the following types of licenses:

- Free trial license
- Purchased license

Free trial license

When you install FortiClient EMS, the free trial license is enabled by default. The free trial license supports ten FortiClient endpoints. FortiClient EMS consumes one license count for each managed FortiClient device.

Purchased license

Each purchased license allows management of one FortiClient endpoint. You must purchase a minimum of 100 endpoint licenses, and you can have these EMS licenses for a maximum three year term. You can specify the number of endpoints and the term duration at time of purchase.

You can use a licensed FortiClient EMS to deploy, provision, and manage FortiClient endpoints. However, if you have a FortiGate in your network, you can buy an add-on FortiGate endpoint license to enforce endpoint compliance on the firewall while EMS is managing the endpoints. Using FortiGate with EMS is optional.

An email is sent when you are running out of licenses. Additionally, a log entry is entered when a client is refused connection due to unavailable licenses.

Component applications

Common services or applications do not require a license.

During the installation of common services required for FortiClient EMS, you are not asked for license information.

Required services and ports

You must ensure required ports and services are enabled for use by FortiClient EMS and its associated applications on your server. The required ports and services enable FortiClient EMS to communicate with endpoints and servers running associated applications. You do not need to enable ports 8013 and 10443 as the FortiClient EMS installation opens these.

Communication	Service	Protocol	Port
FortiClient endpoint/FortiClient Telemetry	File transfers	TCP	8013 (default)
FortiClient big data communication • Used for FortiClient to upload large amounts of data (100+ KB of data per connection) to FortiClient EMS.	File transfers	TCP	8014 (default)
Computer browser service • Allows FortiClient endpoints to automatically connect to EMS. The computer browser service is not needed if an Active Directory is used or endpoint users can manually connect FortiClient to EMS.	Enabled		
Samba (SMB) service • FortiClient EMS uses the SMB service during FortiClient deployment.	Enabled		445

Communication	Service	Protocol	Port
Distributed Computing Environment / Remote Procedure Calls (DCE- RPC) • The EMS server connects to endpoints using RPC for FortiClient deployment.	Enabled		135
Active Directory server connection	When used as a default connection		389 (LDAP) or 636 (LDAPS)
FortiClient download	Enabled		10443 (default)
Apache	HTTPS	TCP	443
SQL server			

Ensure the computer browser service is running. On Windows Server 2012 R2, the service is disabled by default. If this service is not active, FortiClient EMS cannot detect computers on the same network, even if they are available.

Management capacity

FortiClient EMS is intended for use by enterprises. It has the capacity to manage a large number of endpoints. The following are suggested host system hardware configurations for FortiClient EMS. The suggested configurations depend on the number of endpoints FortiClient EMS is managing.

You need at least 200 GB of disk space available.

Maximum number of managed endpoints	Number of virtual CPUs	Memory (RAM) (in GB)	Suggested keep alive interval
10000	2	8	Default
20000	4	8	Default
30000	4	8	120 seconds
40000	4	8	120 seconds
50000	4	8	120 seconds
Suggested minimum system hardware for FortiClient EMS:			
75000	8	16	120 seconds

For the purpose of this table, an Intel i5 processor with two cores and two threads per core is considered to have four virtual CPUs. An Intel i3 processor with two cores and one thread per core has two virtual CPUs.

Server readiness checklist for installation

Use the following checklist to prepare your server for installation.

Checklist	Readiness factor
	Temporarily disable security applications. You must temporarily disable any antivirus software on the target server before you install FortiClient EMS. Installation may be slow or disrupted while these programs are active. Note a server may be vulnerable to attack when you uninstall or disable security applications.
	Consider the date and time settings you apply to your server.
	Confirm required services and ports are enabled and available for use by FortiClient EMS.
	Ensure no conflict exists with port 443 for the Apache service to function properly.
	Ensure no conflict exists with port 8013 for the EMS service to function properly.

Upgrading from an earlier FortiClient EMS version

FortiClient EMS 1.2.3 supports upgrading from FortiClient EMS 1.0.3 and later 1.0 versions. To ensure a successful upgrade, it is recommended you perform the upgrade on a staging server before upgrading the production server. Follow the procedure below.

1. (Optional) Back up the database from the EMS 1.0.x production server.
2. Install EMS 1.0.x on a staging server.
3. (Optional) Import the EMS 1.0.x database from the production server.
4. Connect FortiClient endpoints to the staging server.
5. Upgrade the staging server to EMS 1.2.3.
6. Monitor the staging server for two days.
7. Upgrade the production server to EMS 1.2.3.

Installation and Licensing

Before you install and license FortiClient EMS on a server, ensure you have:

- Reviewed Licenses on page 24
- Met the requirements listed in Required services and ports on page 25
- Completed the Server readiness checklist for installation on page 27
- Logged into the server as the administrator. The administrator user account is equivalent to a Windows administrator account and provides access to all common services, FortiClient EMS, and other application tasks. You can use this account to initially log into the server and to create other user accounts for normal day-to-day use of the applications.

It is recommended you install FortiClient EMS on a dedicated server in a controlled environment. Installing other software applications can interfere with normal operation of FortiClient EMS.

Downloading the installation file

FortiClient EMS is available for download from the following location:

Fortinet Support website: https://support.fortinet.com/

You can also receive the installation file from a sales representative.

The following installation file is available for FortiClient EMS:

`FortiClientEnterpriseManagement_1.2.3.<build>_x64.exe`

For information about obtaining FortiClient EMS, contact your Fortinet reseller.

Installing FortiClient EMS

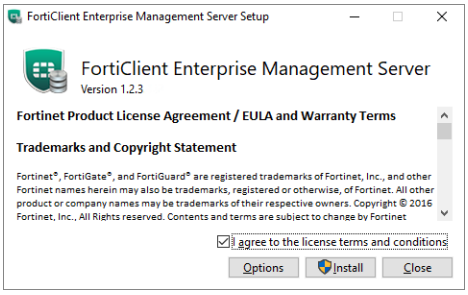
The FortiClient EMS installation package includes:

- FortiClient EMS
- Microsoft SQL Server 2014 Express Edition
- Apache HTTP server

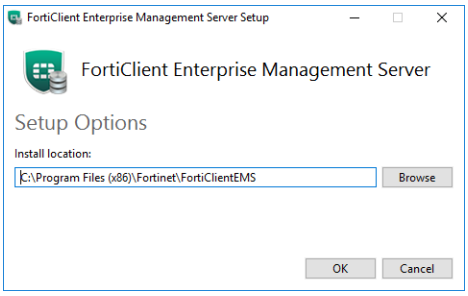
Local administrator rights and Internet access are required to install FortiClient EMS.

To install FortiClient EMS:

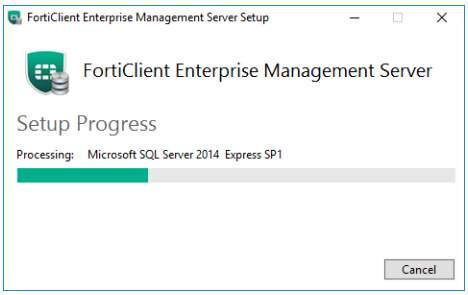
1. If you are logged into the system as an administrator, double-click the downloaded installation file.
   If you are not logged in as an administrator, right-click the installation file, and select *Run as administrator*.
2. If applicable, select *Yes* in the *User Account Control* window to allow the program to make changes to your system.
3. In the installation window, select *I agree to the license terms and conditions* if you agree with the license terms and conditions. If you do not agree, you cannot install the software.



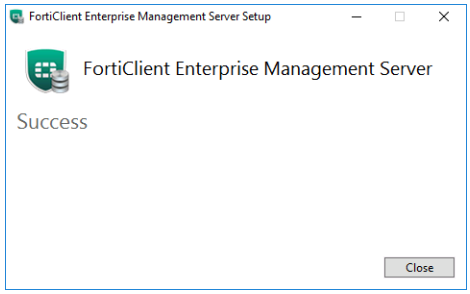
4. (Optional) Click *Options* to specify a custom directory for the FortiClient EMS installation.



   a. Click *Browse* to locate and select the custom directory.
   b. Click *OK* to return to the installation wizard.
5. Click *Install*.
   The installation may take 30 minutes or longer. It may appear to stop at times, but this is only because certain steps in the installation process take longer than others.



6. When the program has installed correctly, the *Success* window displays. Click *Close*.



A *FortiClient Enterprise Management Server* icon is added to the desktop.

Starting FortiClient EMS and logging in

FortiClient EMS runs as a service on Windows computers.

To start FortiClient EMS:

1. Double-click the *FortiClient Enterprise Management Server* icon.
2. Sign in with the username *admin* and no password.
3. Change the username and password by going to *Administration* > *Administrators*.
4. Configure FortiClient EMS by going to *System Settings*.

Accessing FortiClient EMS remotely

You can access FortiClient EMS remotely using a web browser instead of the GUI.

To enable remote access to FortiClient EMS:

1. Go to *System Settings* > *Server*.
2. Enable *Remote HTTPS access*.
3. If desired, in the *Custom hostname* box, type the host name or IP address. Otherwise, the *Pre-defined hostname* is used.
4. If desired, select the *Redirect HTTP request to HTTPS* checkbox. If this option is enabled, if you attempt to remotely access EMS at *http://<server_name>*, this is automatically redirected to *https://<server_name>*.
5. Click *Save*.

To remotely access FortiClient EMS:

- To access EMS from the EMS server, visit `https://localhost`
- To access the server remotely, use the server's hostname: `https://<server_name>`

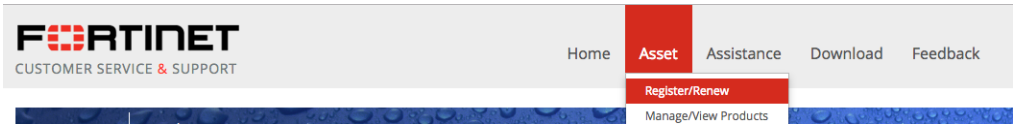
  Ensure you can ping `<server_name>` remotely. This can be achieved by adding it into a DNS entry or to the Windows hosts file. You may have to modify the Windows firewall rules to allow the connection.

Licensing FortiClient EMS

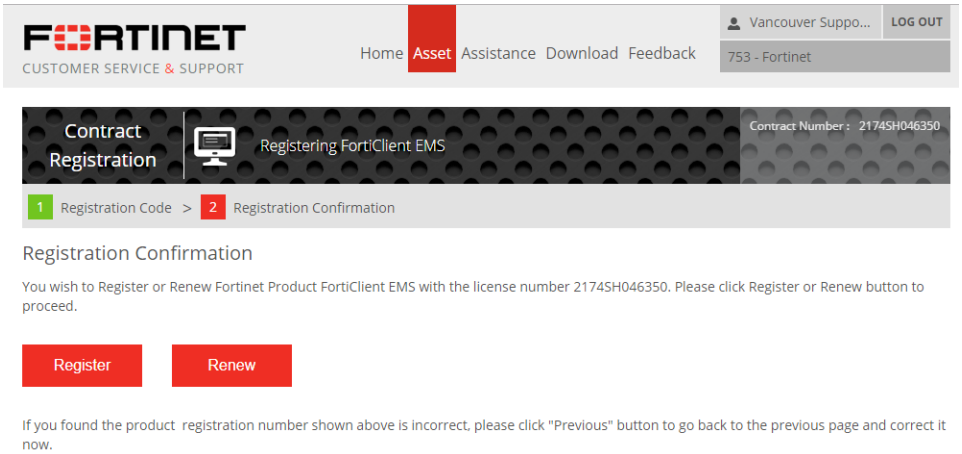
An instructional video on how to obtain licensing for FortiClient EMS is available in the Fortinet Video Library.

To license FortiClient EMS:

1. Purchase FortiClient EMS from a reseller.
   You can visit fortinet.com/partners.html to find a reseller. Once you purchase FortiClient EMS, you receive the *Service Registration Document* via email. This email contains the *Contract Registration Code* used to obtain the FortiClient EMS license.
2. Log into the Fortinet Support website.
3. Register FortiClient EMS:
   a. Go to *Asset* > *Register/Renew*.



   b. In the *Specify Registration Code* field, enter the *Contract Registration Code*. This is the number received in the license email from Fortinet.
   c. Select the end user type, then click *Next*.
   d. Click *Register*.

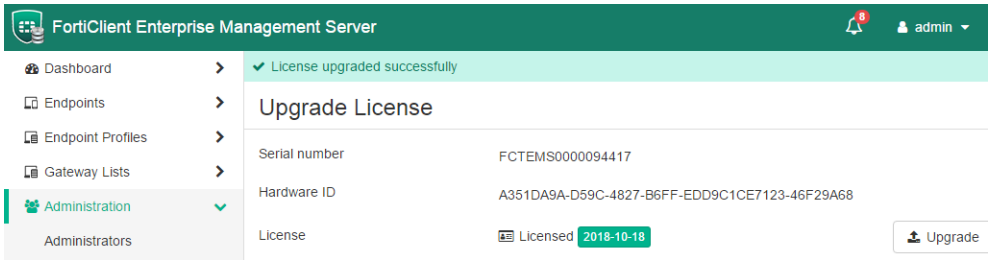


   If you have not registered an EMS device, you are prompted to do so. This requires obtaining the *Hardware ID* from FortiClient EMS. You can obtain the *Hardware ID* by going to *Administration* > *Upgrade License* > *Hardware ID*.
   e. In the *Product Description* field, enter a product description if desired, then enter the *Hardware ID*.
   f. Select the *Fortinet Partner* reseller, then click *Next*.
   g. Read, verify, and agree to the service's *Terms and Conditions*, then click *Next*.
   h. Verify the *Product Entitlement* list for your FortiClient EMS purchase. Select the *BY ACCEPTING THESE TERMS...* checkbox, then click *Confirm*. The license file is now available to use with your FortiClient EMS

installation.

i. Click *Finish*.

4. Retrieve the license key:
   a. Go to *Asset* > *Manage/View Products*. Select FortiClient EMS.
   b. From the left panel, select *License & Key*.
   c. From the *Available Key(s)* list, click *Get The License File* for FortiClient EMS.
5. License FortiClient EMS:
   a. From FortiClient EMS, go to *Administration* > *Upgrade License*. Click the *Activate* button.
   b. Click the *Browse* button, select the license file, and click *Upload*. You have successfully licensed FortiClient EMS.



To upgrade or renew your license, contact Fortinet Support.

License status

The *Dashboard* > *FortiClient Status* > *System Information* widget displays your license status. Your license status can change. The options are:

License Status	Description
Trial	If you just installed FortiClient EMS, the trial license is enabled by default. You should upload the license file you purchased.
Non-expired license	You can upgrade the license. See License upgrades or renewals on page 104.
Expired license	You can renew the license. See License upgrades or renewals on page 104.

Extending license expiries

You can apply multiple licenses to FortiClient EMS to extend the license expiry. For example, consider you purchase two one-year licenses for FortiClient EMS. After you register and apply the first license, FortiClient EMS has an expiry date of September 5, 2018. You can register and apply the second license as a renewal, after which FortiClient EMS has an expiry date of September 5, 2019.

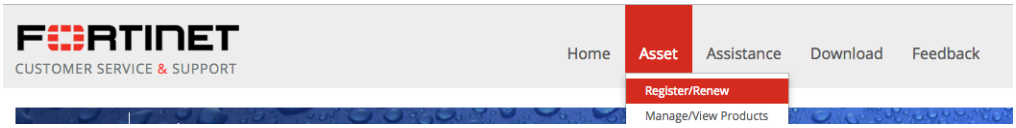
Note you must upload the second license file to FortiClient EMS using the GUI. Registering the license does not automatically update the license expiry in FortiClient EMS.

Using a second license to extend the license expiry date does not increase the number of licensed clients. To increase the number of licensed clients, contact Fortinet Support for a co-term contract.

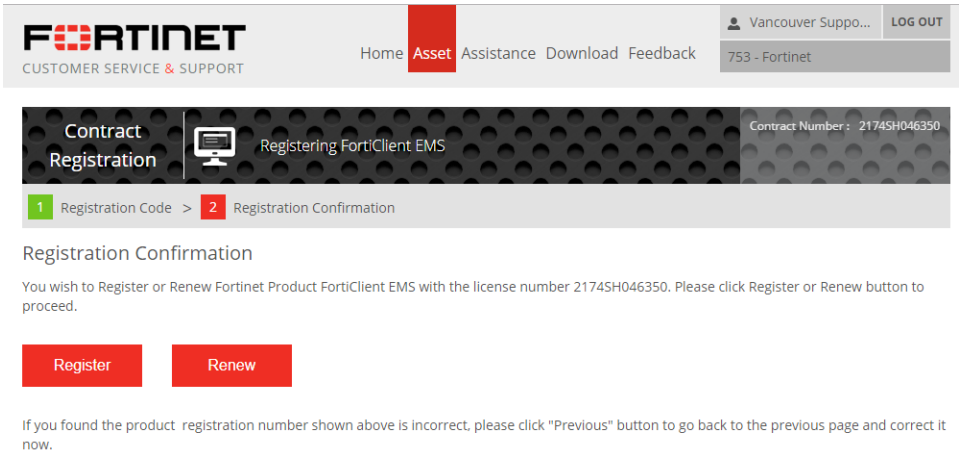
To extend a license expiry:

1. Purchase two FortiClient EMS licenses separately from a reseller. You must purchase the licenses separately to ensure there are two registration codes. Otherwise, you cannot stack the licenses.

   You can visit fortinet.com/partners.html to find a reseller. Once you purchase FortiClient EMS, you receive the *Service Registration Document* via email. This email contains the *Contract Registration Code* used to obtain the FortiClient EMS license.
2. Register and apply the first license to FortiClient EMS as described in Licensing FortiClient EMS on page 31.
3. Register the second license:
   a. Log into the Fortinet Support website.
   b. Go to *Asset* > *Register/Renew*.

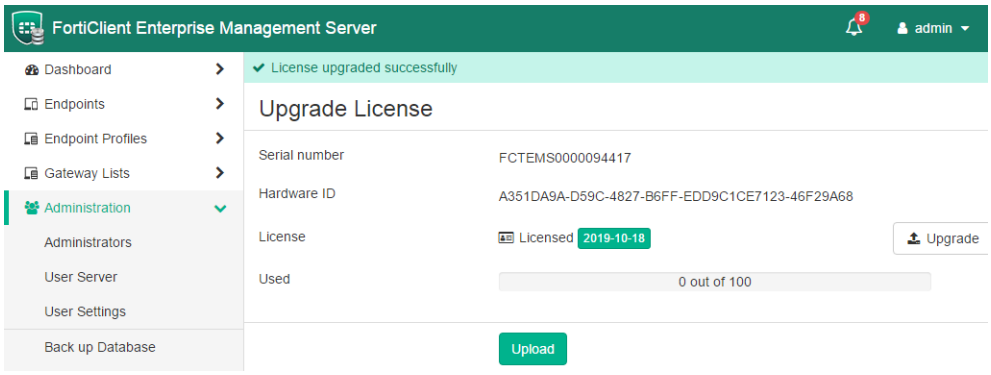


   c. In the *Specify Registration Code* field, enter the *Contract Registration Code*. This is the number received in the license email from Fortinet.
   d. Select the end user type, then click *Next*.
   e. In the *Registration Confirmation* window, click *Renew*.



   f. In the *Specify Fortinet Registration Information* window, do one of the following. You can find the serial number in the *System Information* widget in FortiClient EMS.
      i. Enter the serial number in the *The Product Serial Number is* field.
      ii. Select the desired serial number in the *Product SN* list.
   g. Read, verify, and agree to the service's *Terms and Conditions*.
4. Retrieve the license key:
   a. Go to *Asset* > *Manage/View Products*. Select FortiClient EMS.
   b. From the left panel, select *License and Key*.
   c. From the *Available Key(s) List*, select the FortiClient EMS entry. Then, click *Get The License File*.

5. License FortiClient EMS:
   a. From FortiClient EMS, go to *Administration* > *Upgrade License*, then click *Activate*.
   b. Click *Browse*, select the license file, and click *Upload*. You have successfully extended the license for FortiClient EMS. The expiry date displayed in the *System Information* widget updates to a year after the initial license expiry date.



Help with licensing

For licensing issues with FortiClient EMS, contact the licensing team at Fortinet Technical Assistance Center (TAC):

- Phone: +1-866-648-4638
- Technical support: support.fortinet.com/

Specifying different ports

In cases where there are pre-existing services running on default FortiClient EMS ports, you can specify another port using the CLI to run the installer. You can use the following commands:

Command	Description
`ClientDownloadPort`	Port used to download FortiClient from FortiClient EMS.
`RemoteManagementPort`	Port used for EMS administration.

Upgrading Microsoft SQL Server Express to Microsoft SQL Server Standard or Enterprise

FortiClient EMS is installed with Microsoft SQL Server Express, which has a file size limit of 10 GB per database. Log entries recorded in the database are rotated on a schedule of seven days (one week) by default. If the FortiClient deployment is large, the database size may reach the 10 GB limit over time. The FortiClient EMS administrator may upgrade SQL Server from Express to Standard or Enterprise edition. The database file size limit for these editions is in the PB range, which is unlimited for most practical usage.

Microsoft SQL Server Express is free. All other editions require a license from Microsoft.

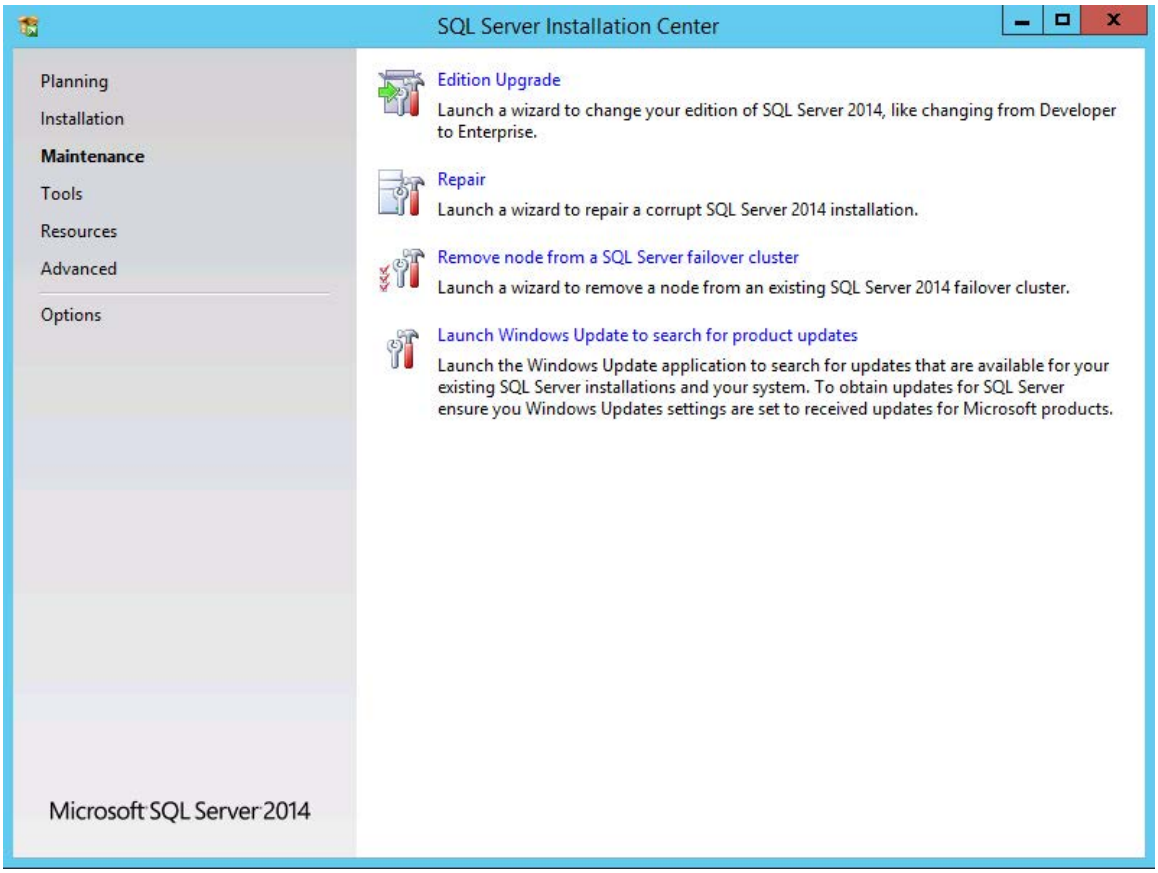
See the following Microsoft documentation on upgrading between editions called *Upgrade to a Different Edition of SQL Server 2014 (Setup)* at https://technet.microsoft.com/en-us/library/cc707783(v=sql.120).aspx

The EMS database is saved in the *C:\Program Files\Microsoft SQL Server\MSSQL12.FCEMS\MSSQL\DATA\FCM_root.mdf* file in the EMS host server. This file's size should remain below the 10 GB limit for Microsoft SQL Server Express.

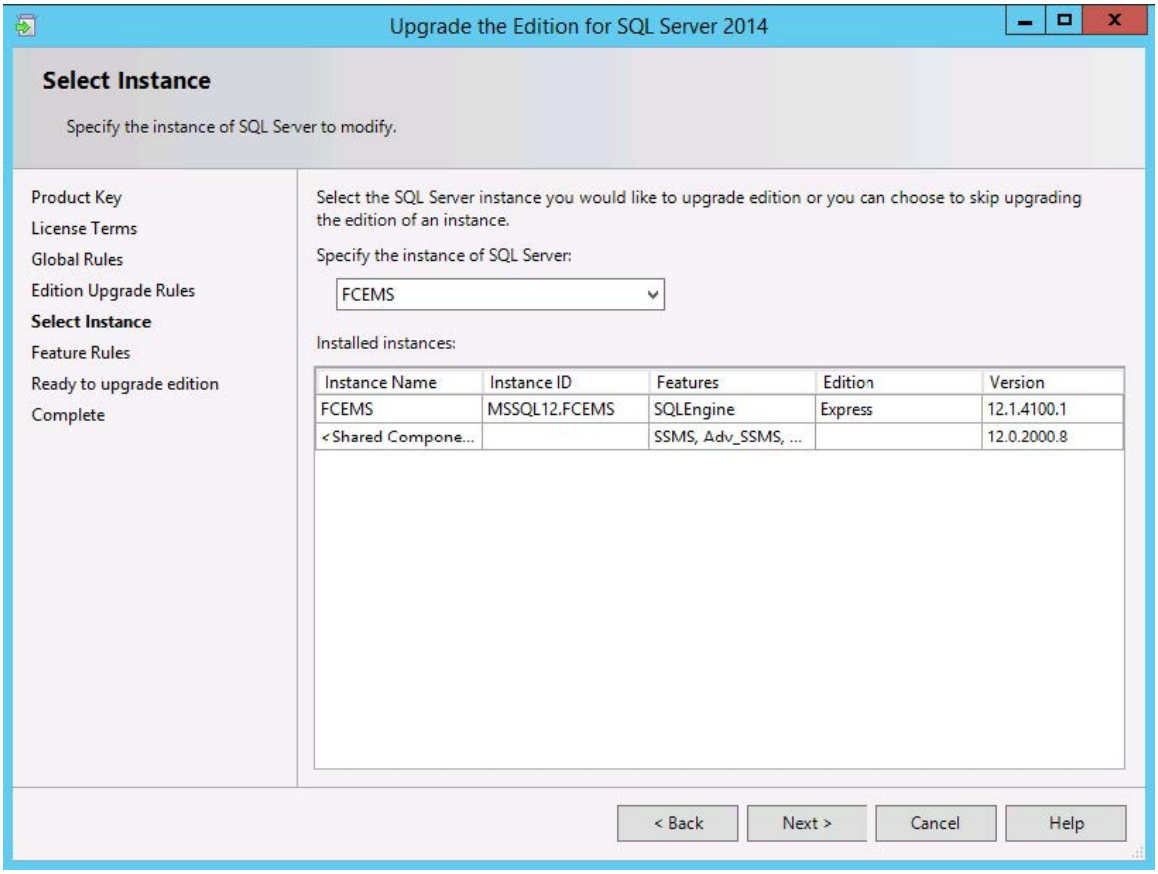
It is recommended to do a database edition upgrade outside normal production hours.

To upgrade Microsoft SQL Server Express:

1. Attach the SQL Server 2014 installation media to the FortiClient EMS server.
   The installation media is a DVD or ISO file. If using the DVD, insert the DVD into the EMS host computer (host server). If your host server is a virtual machine, use the ISO file.
2. Run the SQL Server setup application wizard.
3. In the *SQL Server Installation Center* wizard, go to *Maintenance* > *Edition Upgrade*.



4. Enter the *product key*.
5. Accept the license terms, then click *Next*.
6. Under *Select Instance*, in the *Specify the instance of SQL Server* dropdown list, select *FCEMS*. Then, click *Next*.



7. Under *Ready to upgrade edition*, click *Upgrade*.
8. After the upgrade is complete, click *Finish*.

Testing the SQL server upgrade

It is recommended to run a short test on FortiClient EMS after the upgrade to verify proper operations. A simple test may be to:

1. Connect FortiClient on one or two test endpoints to FortiClient EMS.
2. Create a new custom group in FortiClient EMS and add the test endpoints to it.
3. Create a new endpoint profile and assign it to the new custom group.
4. Check that FortiClient on the test endpoints received the new profile.

Monitor the system closely over the first few days for any unusual behavior.

Uninstalling FortiClient EMS

Use the *Programs and Features* pane of the Microsoft Windows Control Panel to uninstall FortiClient EMS.

FortiClient EMS installs the following dependencies. If other applications on the same computer are not using them, you can uninstall them manually after removing FortiClient EMS.

- Microsoft ODBC Driver 11 for SQL Server
- Microsoft SQL Server 2008 Setup Support Files
- Microsoft SQL Server 2012 Native Client
- Microsoft SQL Server 2014 (64-bit)
- Microsoft SQL Server 2014 Setup (English)
- Microsoft SQL Server 2014 Transact-SQL ScriptDom
- Microsoft Visual C++ 2010 x64 Redistributable – 10.0
- Microsoft Visual C++ 2010 x86 Redistributable – 10.0
- Microsoft Visual C++ 2013 x86 Redistributable – 12.0
- Microsoft VSS Writer for SQL Server 2014
- SQL Server Browser for SQL Server 2014

To uninstall FortiClient EMS:

1. Select *Start* > *Control Panel* > *Programs* > *Uninstall a program*.
2. Select *FortiClient Enterprise Management Server*, and click *Uninstall*.
3. Follow the uninstallation wizard prompts.

GUI

The FortiClient EMS GUI consists of the following areas:

- Banner
- Left pane
- Content pane

Banner

Option	Description
Bell icon	Click the bell icon to display all alert logs.
<Logged in username>	Click the dropdown list beside the <logged in username> to log out of FortiClient EMS.

Left pane

The left navigation pane is used to display content in the right content pane.

Option		Description
Dashboard		
	FortiClient Status	Displays a dashboard of information about all managed endpoints.
	Vulnerability Scan	Displays the Current Vulnerabilities Summary chart that provides a centralized vulnerability summary for all managed endpoints. You can observe high-risk hosts and critical vulnerabilities existing on endpoints. You can also access links on how to fix or repair the vulnerabilities.
Endpoints		
	All Endpoints	Add and manage all endpoints.
	Manage Domains	Manage domains.
	Domains	Add and manage endpoints from domains.
	Workgroups	Add and manage endpoints from workgroups.
Endpoint Profiles		

Option		Description
	Manage Profiles	Create and assign profiles and manage profile updates for all profiles.
	Local Profiles	Create and assign profiles and manage profile updates for local profiles.
Gateway Lists		Create and assign gateway IP lists and manage IP list updates.
Administration		
	Administrators	Add and manage administrators.
	User Server	Configure the user server.
	User Settings	Configure the inactivity timeout.
	Back up Database	Back up the FortiClient EMS database.
	Restore Database	Restore the FortiClient EMS database.
	Upgrade License	Upgrade or renew the FortiClient EMS license.
	Software Management	Add and manage FortiClient installers.
	CA Certificate Management	Import CA certificates into FortiClient EMS.
	Logs	View log messages generated by FortiClient EMS and download raw logs.
System Settings		
	Server	Change the IP address and port and configure other server settings for FortiClient EMS.
	Logs	Specify what level of log messages to capture in FortiClient EMS logs and when to automatically delete logs and alerts.
	FortiGuard	Configure FortiGuard settings.
	Endpoints	Configure endpoint settings.
	Login Banner	Enable the pre-login banner to display a message to a user logging into FortiClient EMS.
	EMS Alerts	Enable alerts for FortiClient EMS events.
	Endpoint Alerts	Enable alerts for endpoint events.
	SMTP Server	Set up an SMTP server to enable email alerts.
Help		
	Getting Started	Provides access to links to the FortiClient EMS *Release Notes*, *QuickStart Guide*, and other resources.

Option		Description
	Technical Documentation	Link to the FortiClient EMS documentation.
	How-To Videos	Link to the Fortinet Video Library website.
	Forums	Link to Fortinet Customer Service and Support forum.
	Introduction to FortiClient EMS	Link to an introductory video for FortiClient EMS, which gives an overview of features, modes, and system requirements for FortiClient EMS 1.0.
	How to License FortiClient EMS	Link to a video showing how to license or renew FortiClient EMS 1.0 with more endpoints.
	Adding a Domain to FortiClient EMS	Link to a video showing how to add an Active Directory domain to FortiClient EMS.
	Create Support Package	Create a support package to provide to the Fortinet technical support team for troubleshooting.
	FortiGuard	View list of engine and signature versions for this version of FortiClient EMS.

Content pane

The right content pane displays the user interface controls that correspond to the selection made in the left pane. The status and menu icons in the top-right display controls what you can use to configure additional settings for user management and each individual endpoint.

Dashboard

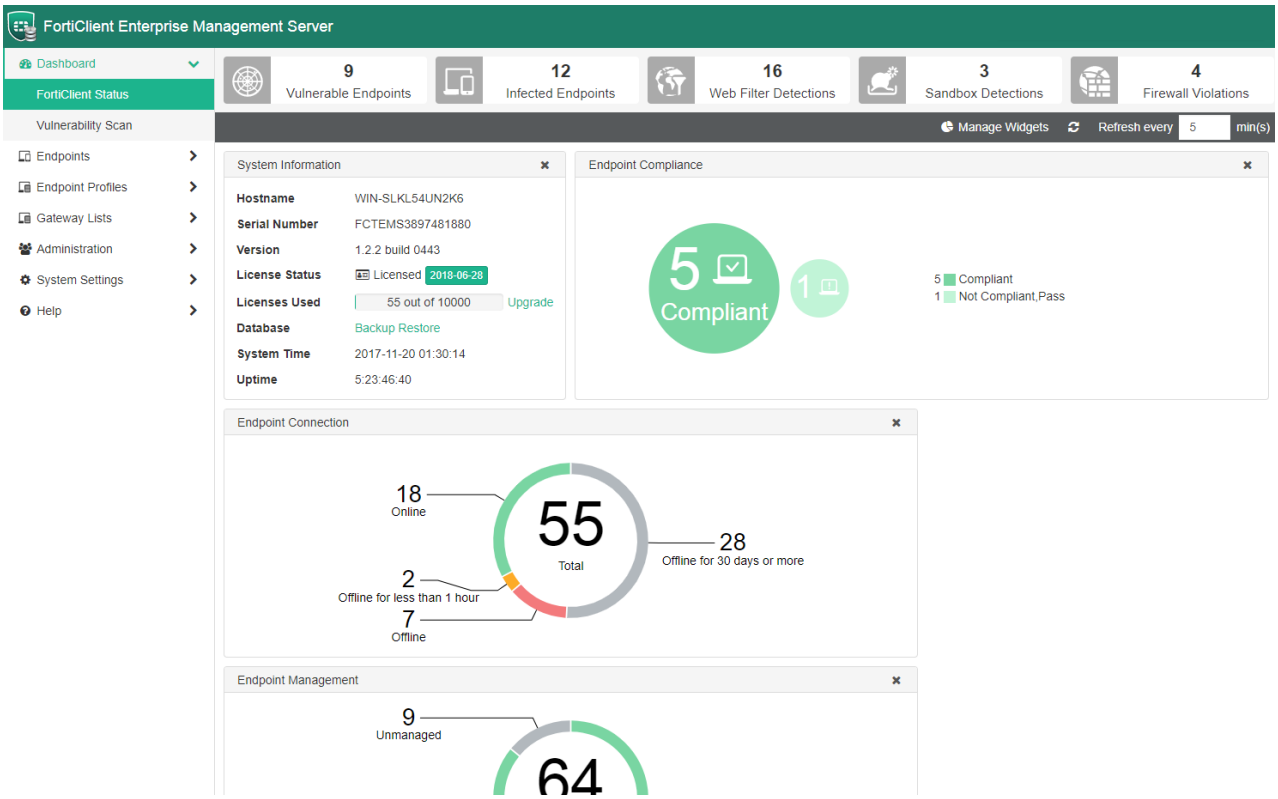
You can use the Dashboard to view summary information about the system and endpoints. You can view summary information about vulnerability scans on endpoints.

- Viewing the FortiClient Status on page 41
- Viewing the Vulnerability Scan dashboard on page 44

Viewing the FortiClient Status

To view the FortiClient Status:

1. In the left pane, click *Dashboard* > *FortiClient Status*.
   A *System Information* widget and charts and widgets of summary information display. See System Information widget on page 42 and FortiClient Status charts and widgets on page 42.



2. Click an event summary.
   The list of endpoints for the summary displays.
3. Click the *Back* button to return to the *FortiClient Status* pane.

4. Click a pie chart.
   The *Endpoints* content pane displays with more details about the endpoints related to the pie charts. See also Viewing the Endpoints content pane on page 51.

System Information widget

The following information displays in the *System Information* widget:

Option	Description
Hostname	Name of the computer on which FortiClient EMS is installed.
Serial Number	Serial number for FortiClient EMS.
Version	Version number for FortiClient EMS.
License Status	Status of the license for FortiClient EMS. Also displays a button for activating, upgrading, or renewing a license, depending on the license status. If you have just installed EMS, click *Activate* to upload your license file. If you have a non-expired license, but want to upgrade your license, click the *Upgrade* button to upgrade your license file. If your current license is expiring, the *Renew* button is enabled for you to upload your new license file. See Licensing FortiClient EMS on page 31.
Licenses Used	Number of licenses used out of the total number of available licenses.
Database	Options to back up and restore the database. Click *Backup* to back up the database. Click *Restore* to restore a backed up database.
System Time	Time and date used by the computer on which FortiClient EMS is installed.
Uptime	Number of days, hours, minutes, and seconds FortiClient EMS has been running.

FortiClient Status charts and widgets

FortiClient Status displays a number of pie charts. Each pie chart provides a summary of endpoint information. The sections in each chart are links. You can click any section of the pie charts or any row in the table to display more details.

Option	Description
Endpoint Charts	
Endpoint Activity	Shows a summary of endpoint activity information. Categories are: • FortiGate On-net • FortiGate Off-net • FortiGate Offline • FortiGate Not Registered • EMS On-net • EMS Off-net

Option	Description
Endpoint Alerts	Shows the number of endpoints with alerts, including pending software updates, out-of-date protection, and out-of-sync profiles.
Endpoint Compliance	Shows the number of endpoints that are: • Compliant • Not Compliant, Pass • Not Compliant, Blocked • Not Compliant, Warning
Endpoint Connection	Shows the number of endpoints that are: • Online • Offline for less than one hour • Offline • Offline for 30 days or more
FortiClient Versions	These chart indicates the percentage of endpoints with each version of FortiClient installed. There is one chart for FortiClient (Windows) versions and another chart for FortiClient (Mac OS X) versions.
Endpoint Management	This chart indicates how many endpoints are unregistered and registered.
Operating Systems	This chart indicates the number of endpoints running each version of Windows and Mac operating systems. There is one chart for Windows OS versions and another chart for Mac OS versions.
Endpoint Telemetry & Fabric	This chart indicates how many endpoints are connected to each FortiGate. It also indicates the number of endpoints not participating in the Security Fabric.
Top 3 Lists	
Antivirus Detection	This chart indicates the top three endpoints with antivirus alerts, including the number of antivrus alerts for each endpoint.
Sandbox Detection	This chart indicates the top three endpoints with FortiSandbox alerts, including the number of FortiSandbox alerts for each endpoint.
Vulnerability Detection	This chart indicates the top three endpoints with antivirus alerts, including the number of antivirus alerts for each endpoint.
Web Filter Detection	This chart indicates the top three endpoints with web filter alerts, including the number of web filter alerts for each endpoint.
Others	
System Information	This widget displays summary information for the system.

Viewing the Vulnerability Scan dashboard

To view the Vulnerability Scan dashboard:

1. In the left pane, click *Dashboard* > *Vulnerability Scan*. Charts and widgets display a summary of vulnerability scan information.
2. Click a pie chart to view details about the vulnerabilities.

Vulnerability Scan charts and widgets

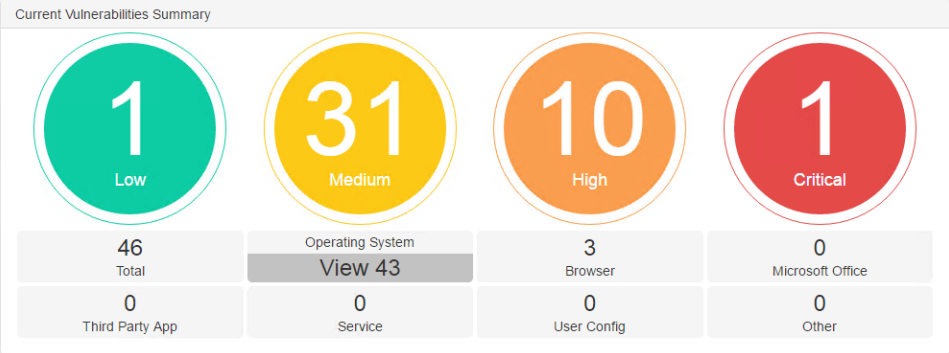
The *Vulnerability Scan* dashboard displays a number of pie charts. Each pie chart provides a summary of endpoint information. The sections in each chart are links. You can click any section of the pie charts or any row in the table to display more details.

Option	Description
Current Vulnerabilities Summary	Displays the following summaries of current vulnerabilities: • Total (total number of vulnerabilities) • Operating System (number of operating system vulnerabilities) • Browser (number of browser vulnerabilities) • Microsoft Office (number of Microsoft Office vulnerabilities) • Third Party App (number of third-party application vulnerabilities) • Service (number of service vulnerabilities) • User Config (number of user configuration vulnerabilities) • Other (number of other vulnerabilities that do not fit any of the above categories) When you click a vulnerability tile, the severity of vulnerabilities displays in the colored circles above.
Endpoint Scan Status	Displays the following summaries about endpoints: • Vulnerable Endpoints • Un-Scanned Endpoints • Secured Endpoints • Scanning Endpoints
Top 10 Vulnerable Endpoints	Displays the top ten vulnerable endpoints and the number of vulnerabilities within that endpoint.
Top 10 Vulnerabilities	Displays the top ten vulnerabilities.

Viewing current vulnerabilities

To view current vulnerabilities:

1. Click a vulnerability tile.
2. The colored circles change and display the number of vulnerabilities and severities corresponding to the selected *Vulnerability Tile*.



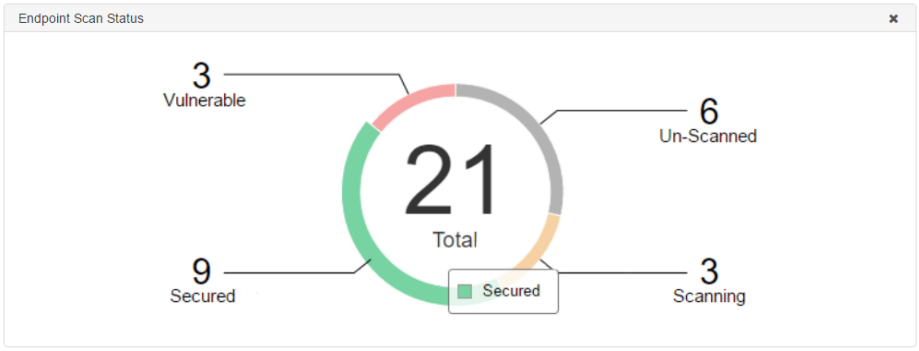
For example, click the *Operating System* tile, which has a total of 46 *Vulnerabilities*. The *Vulnerabilities* are organized by *Severity*:

- 1/62 is *Low Risk* (green circle)
- 31/62 are *Medium Risk* (yellow circle)
- 10/62 are *High Risk* (orange circle)
- 1/62 is *Critical Risk* (red circle)

Viewing the Endpoint Scan Status

To view the Endpoint Scan Status:

1. Click a section of the *Endpoint Scan Status* chart.
   The Endpoint content pane displays with information about the endpoints corresponding to the section.



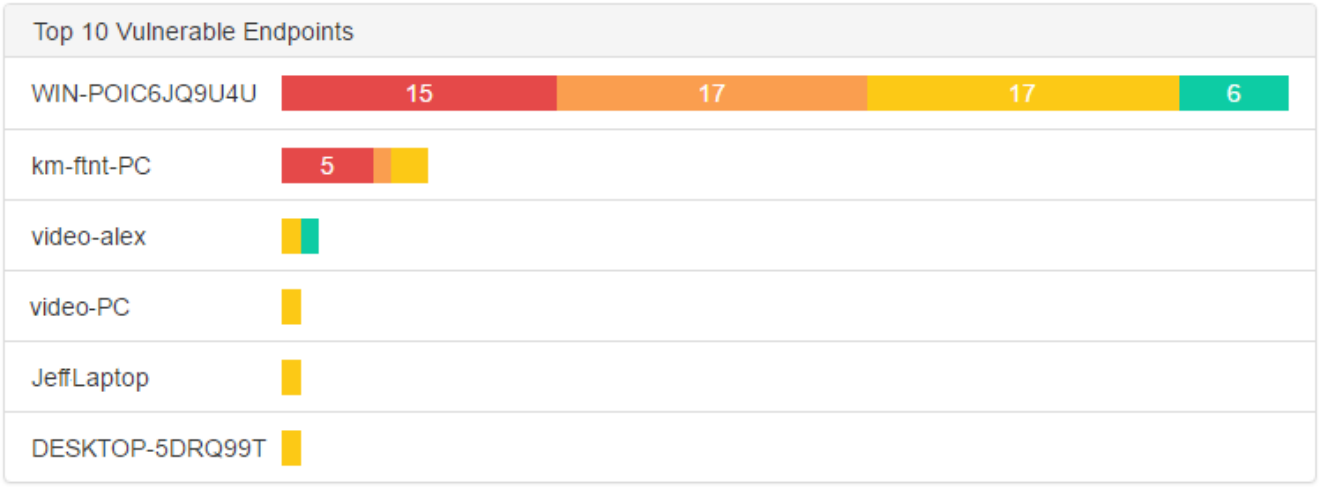
For example, click the *Secured Endpoints* section, which has a total of 21 *Endpoints*. The *Endpoints* are organized by type:

- 9/21 are *Secured* (green section)
- 3/21 are *Vulnerable* (red section)

- 6/21 are *Un-Scanned* (yellow section)
- 3/21 are *Scanning* (grey section)

Viewing top ten vulnerabilities on endpoints

How to read the Top 10 Vulnerable Endpoints widget:

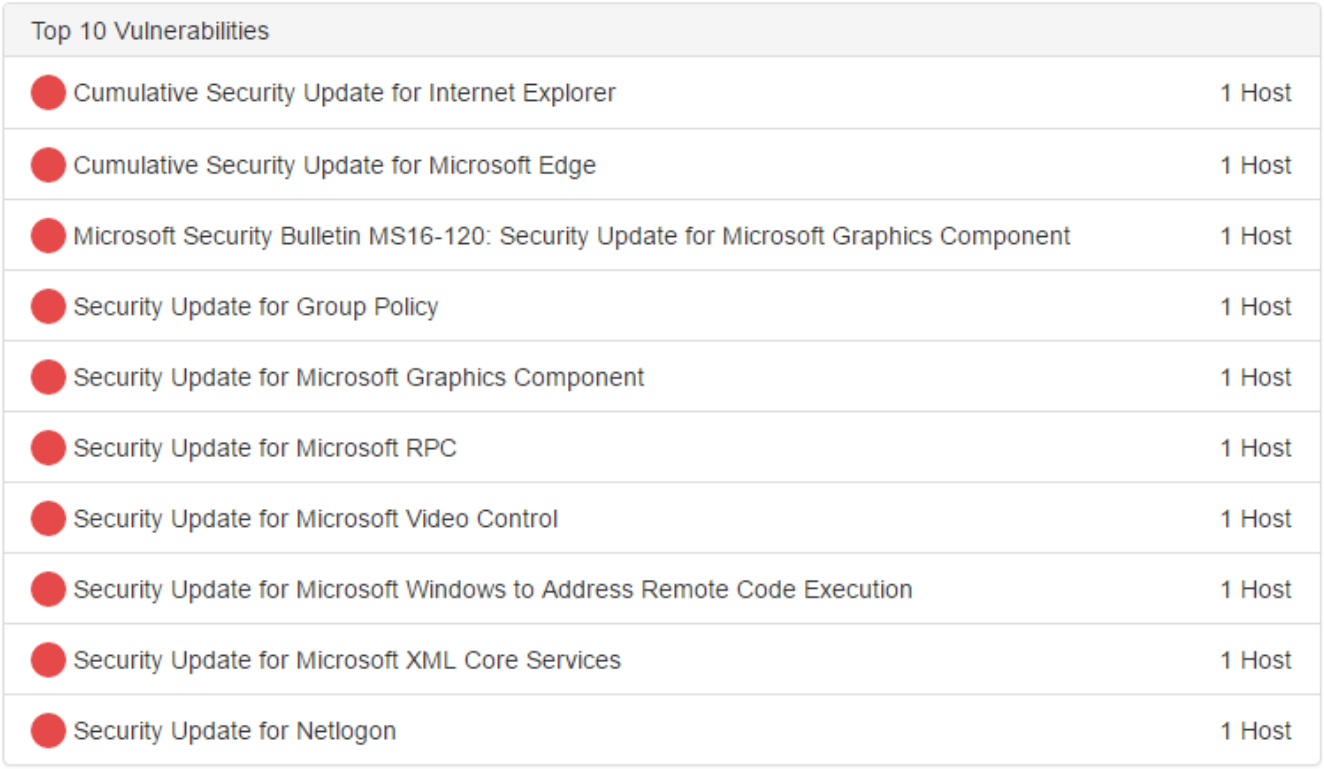


For example, the *Top 10 Vulnerable Endpoints* vulnerabilities displays. The *Vulnerabilities* are shown in a segmented bar graph and organized by severity:

WIN-POIC6JQ9U4U has the following:

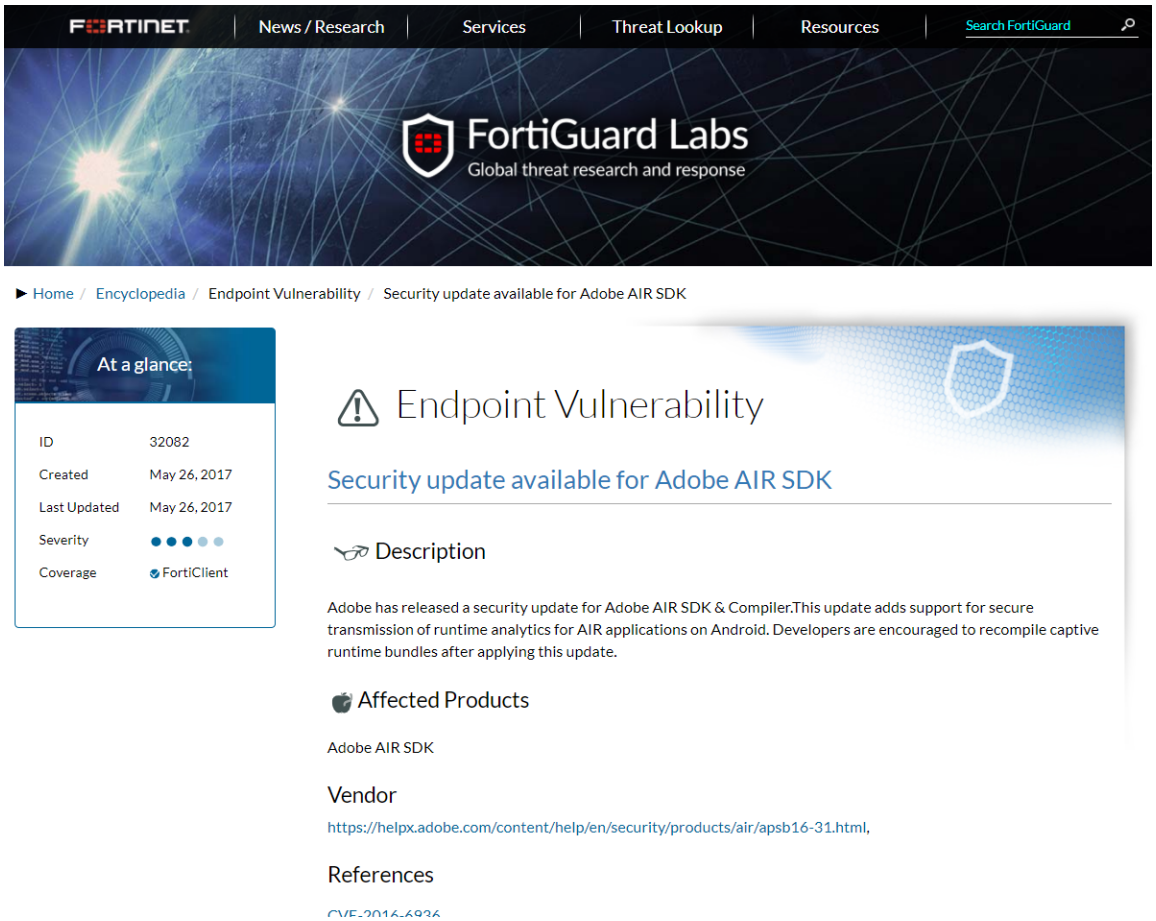
- 15 *Critical Vulnerabilities* (red bar)
- 17 *High Risk Vulnerabilities* (orange bar)
- 17 *Medium Risk Vulnerabilities* (yellow bar)
- 6 *Low Risk Vulnerabilities* (green bar)

How to read the Top 10 Vulnerabilities widget:



The *Top 10 Vulnerabilities* widget displays the type of vulnerability and how many hosts have the vulnerability. For example, the *Cumulative Security Update for Internet Explorer Vulnerability* has one host affected.

When you click a vulnerability, you are redirected to the *FortiGuard Labs Threat Encyclopedia* where details about the vulnerability are available.


FORTINET
News / Research
Services
Threat Lookup
Resources
Search FortiGuard
FortiGuard Labs
Global threat research and response
Home / Encyclopedia / Endpoint Vulnerability / Security update available for Adob AIR SDK
At a glance:
ID 32082
Created May 26, 2017
Last Updated May 26, 2017
Severity
Coverage FortiClient
Endpoint Vulnerability
Security update available for Adobe AIR SDK
Description
Adobe has released a security update for Adobe AIR SDK & Compiler.This update adds support for secure transmission of runtime analytics for AIR applications on Android. Developers are encouraged to recompile captive runtime bundles after applying this update.
Affected Products
Adobe AIR SDK
Vendor
https://helpx.adobe.com/content/help/en/security/products/air/apsb16-31.html,
References

Endpoints

FortiClient EMS needs to determine which devices to manage. Device information can come from an Active Directory server, Windows workgroup, or manual FortiClient connection. You can create groups to organize endpoints.

Creating groups

You can create groups to organize endpoints. You can also rename and delete groups.

To create groups:

1. Go to *Endpoints*.
2. Right-click a domain or workgroup and select *Create group*. The *Create group* dialog box displays.
3. In the *Required* box, type a name for the group, and click *Confirm*.
   The group is created.

To rename groups:

1. Go to *Endpoints*.
2. Right-click the group, and select *Rename group*. The *Rename the group* dialog box displays.
3. In the *Required* box, type the new name, and click *Confirm*.
   The group is renamed.

To delete groups:

1. Go to *Endpoints*.
2. Right-click the group, and select *Delete group*. A confirmation dialog box displays.
3. Click *Yes*.
   The group and any subgroups are deleted.

Adding endpoints

You can add endpoints using an Active Directory service. Endpoints are also added when endpoint users manually connect FortiClient Telemetry to FortiClient EMS.

Adding endpoints using an Active Directory domain server

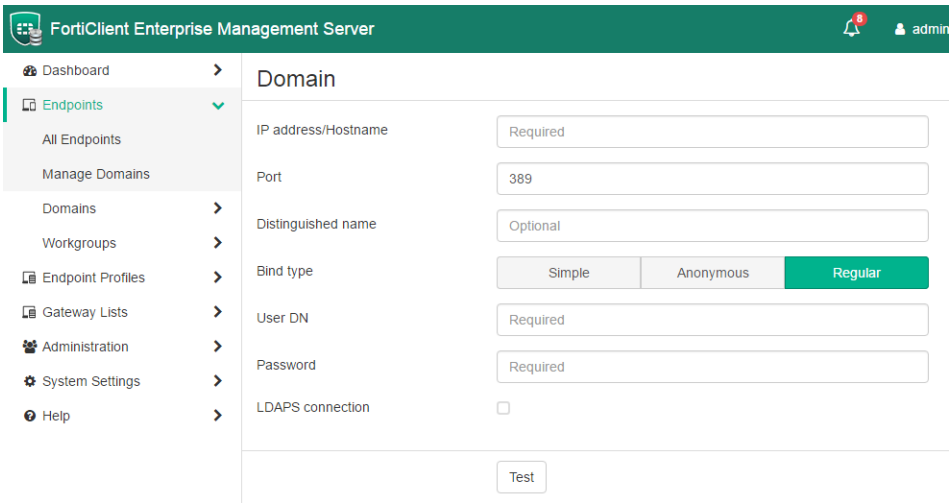
Endpoints can be manually imported from an Active Directory (AD) domain server. You can import and synchronize information about computer accounts with an LDAP or LDAPS service. You can add endpoints by identifying endpoints that are part of an AD domain server.

An instructional video on how to add a domain is available in the Fortinet Video Library.

You can add the entire domain or an organizational unit (OU) from the domain.

To add endpoints using an Active Directory domain service:

1. Click *Endpoints* > *Manage Domains* > *Add*. The *Domain* pane displays.



2. Configure the following options:

IP address/Hostname	Type the IP address or name.
Port	Type the port number.
Distinguished name	Type the distinguished name (optional).
Bind type	Select the bind type: *Simple*, *Anonymous*, or *Regular*. When you select *Regular*, enter the *User DN* and *Password*.
User DN	Available when *Bind Type* is set to *Regular*. Type the user DN.
Password	Available when *Bind Type* is set to *Regular*. Type the user password.

Show Password	Available when *Bind Type* is set to *Regular*. Turn on and off to show or hide the password.
LDAPS connection	Turn on to enable a secure connection protocol when *Bind Type* is set to *Regular*.

3. Click *Test* to test the domain settings connection.
4. If the test is successful, select *Save* to save the new domain. If not, correct the information as required then test the settings again.

Connecting manually from FortiClient

Endpoint users can manually connect FortiClient Telemetry to FortiClient EMS by specifying the IP address for FortiClient EMS in FortiClient Console. This process is sometimes called registering FortiClient to FortiClient EMS.

To connect FortiClient Telemetry to FortiClient EMS:

1. In FortiClient Console on the endpoint, go to the *Compliance* tab.
2. In the *FortiGate or EMS* box, type the IP address for EMS, and click *Connect*.
   FortiClient connects to FortiClient EMS.

For information about FortiClient, see the *FortiClient Administration Guide* available on docs.fortinet.com/forticlient/admin-guides.

The FortiClient Telemetry gateway port may be appended to the gateway IP list address on FortiClient and separated by a colon. When the port is not provided, FortiClient attempts to connect to the IP address given using the default port. The default connection port in FortiClient 5.2 is 8010 and in FortiClient 5.4 is 8013. By default, FortiClient EMS listens for connection on port 8013.

Viewing endpoints

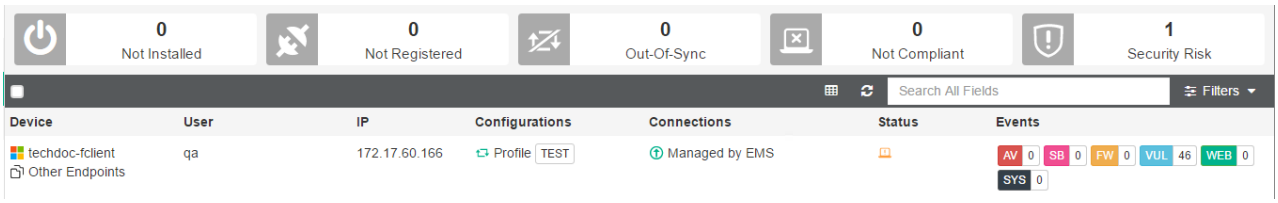
After you add endpoints to FortiClient EMS, you can view the list of endpoints in a domain or workgroup in the *Endpoints* pane. You can also view details about each endpoint in the *Client Details* pane and use filters to access endpoints with specific qualities.

Viewing the Endpoints content pane

You can view information about endpoints on the *Endpoints* content pane.

To view the Endpoints content pane:

1. Go to *Endpoints*, and select *All Endpoints*, a domain, or workgroup.
   The list of endpoints in FortiClient EMS, a quick status bar, and a toolbar display in the content pane.



Not Installed	Number of endpoints that do not have FortiClient installed. Click to display the list of endpoints without FortiClient installed.
Not Registered	Number of endpoints not registered to FortiClient EMS or FortiGate. Click to display the list of unregistered endpoints.
Out-Of-Sync	Number of endpoints with an out-of-sync profile. Click to display the list of endpoints with out-of-sync profiles.
Not Compliant	Number of endpoints not compliant with the FortiGate compliance rules. Click to display the list of not compliant endpoints.
Security Risk	Number of endpoints that are a security risk. Click to display the list of endpoints.
Checkbox	Click to select all endpoints displayed in the content pane.
Show/Hide Heading	Click to hide and display the following column headings: *Device*, *User*, *IP*, *Configurations*, *Connections*, *Status*, and *Events*.
Refresh	Click to refresh the list of endpoints in the content pane.
Search All Fields	Type a value and press *Enter* to search for the value in the list of endpoints.
Filters	Click to display and hide filters you can use to filter the list of endpoints.
Device	Visible when headings are displayed. Displays an icon to represent the operating system on the endpoint and the device name.
User	Visible when headings are displayed. Displays the name of the user logged into the endpoint.
IP	Visible when headings are displayed. Displays the endpoint's IP address.
Configurations	Visible when headings are displayed. Displays the name of the profile assigned to the endpoint and the profile's synchronization status.
Connections	Visible when headings are displayed. Displays whether the endpoint is connected to FortiClient EMS or FortiGate and the connection status of *Online*, *Offline*, or *Not Registered*.

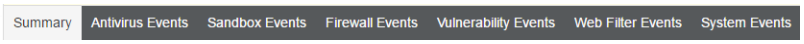
Status	Visible when headings are displayed. Displays one of the following compliance statuses for the endpoint. • Compliant • Not compliant • Not participating in compliance • Quarantined • Excluded • Not registered • Not installed
Events	Visible when headings are displayed. Displays FortiClient events for the endpoint.

2. Click an endpoint to display its details in the content pane.

The following dropdown lists display in the toolbar for the selected endpoint:

Checkbox	Click to select and deselect all endpoints in the content pane. You can then select or clear the checkbox for individual endpoints to fine-tune the list of selected endpoints.
Scan	Click to start a Vulnerability or AntiVirus scan on the selected endpoint.
Patch	Click to patch all critical and high vulnerabilities on the selected endpoint. Choose one of the following options: • Selected Vulnerabilities on Selected Clients • Selected Vulnerabilities on All Affected Clients • All Critical and High Vulnerabilities
Action	Click to perform one of the following actions on the selected endpoint: • Upload FortiClient Logs • Request Diagnostic Results • Update Signatures • Re-register • De-register • Register • Quarantine • Un-quarantine • Exclude from Management • Mark as Uninstalled • Delete Device

The following tabs are available in the content pane toolbar when you select an endpoint:



Summary

	<user name>	Displays the name of the user logged into the selected endpoint. Also displays the user's avatar, email address, and phone number if these are provided to FortiClient on the endpoint. If the user's LinkedIn, Google, Salesforce, or other cloud app account is linked in FortiClient, the username from the cloud application displays.
	Device	Displays the selected endpoint's device name.
	OS	Displays the selected endpoint's operating system and version number.
	IP	Displays the selected endpoint's IP address.
	MAC	Displays the selected endpoint's MAC address.
	Last Seen	Displays the last date and time that FortiClient sent a keep-alive message to EMS. This information is useful if FortiClient is offline because it indicates when the last keep-alive message occurred.
	Location	Displays whether the selected endpoint is onnet or offnet.
	Connection	Displays when the selected endpoint is connected to FortiClient EMS or FortiGate. Also displays the connection status.
	Configuration	Displays the following information for the selected endpoint: • Profile: Name of the profile assigned to the selected endpoint • Installer: Name of the FortiClient installer used for the selected endpoint. Displays *Not Assigned* if no FortiClient installer has been assigned to the selected endpoint. • IP List: Name of the gateway IP list used for the selected endpoint. Displays *Not Assigned* if no gateway IP list has been assigned to the selected endpoint. • FortiClient Version: FortiClient version installed on the selected endpoint.
	Compliance	Displays if the endpoint is compliant. If the endpoint is not compliant, displays the features for which FortiClient is not compliant.
	Features	Displays which features are enabled for FortiClient.
Antivirus Events		
	Date/Time	Displays the antivirus event's date and time.
	Message	Displays the antivirus event's message.
Sandbox Events		
	Date/Time	Displays the sandbox event's date and time.
	Message	Displays the sandbox event's message.
Firewall Events		
	Date/Time	Displays the firewall event's date and time.

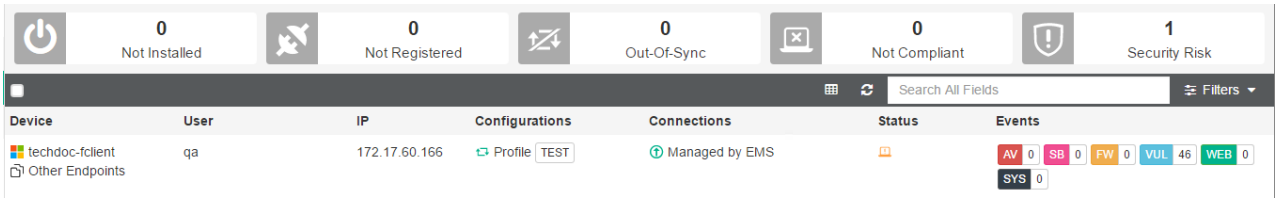
	Message	Displays the firewall event's message.
Vulnerability Events		
	Vulnerability	Displays the vulnerability's name. For example, *Security update available for Adobe Reader*.
	Category	Displays the vulnerability's category. For example, *Third Party App*.
	Application	Displays the name of the application with the vulnerability.
	Severity	Displays the vulnerability's severity.
	FortiGuard ID	Displays the FortiGuard ID number. If you click the FortiGuard ID number, it redirects you to FortiGuard where further information is provided if available.
	Bulletin	Displays a link to a bulletin about the software vulnerability.
Web Filter Events		
	Date/Time	Displays the web filter event's date and time.
	Message	Displays the web filter event's message.
System Events		
	Date/Time	Displays the system event's date and time.
	Message	Displays the system event's message.

Using the quick status bar

You can use the quick status bar to quickly display filtered lists of endpoints on the *Endpoints* content pane.

To use the quick status bar:

1. Go to *Endpoints*.
2. Click *All Endpoints*, a domain, or workgroup.
   The list of endpoints and quick status bar display.



3. Click one of the following buttons in the quick status bar:
   - Not Installed
   - Not Registered
   - Out-Of-Sync
   - Not Compliant
   - Security Risk

The list of affected endpoints displays.

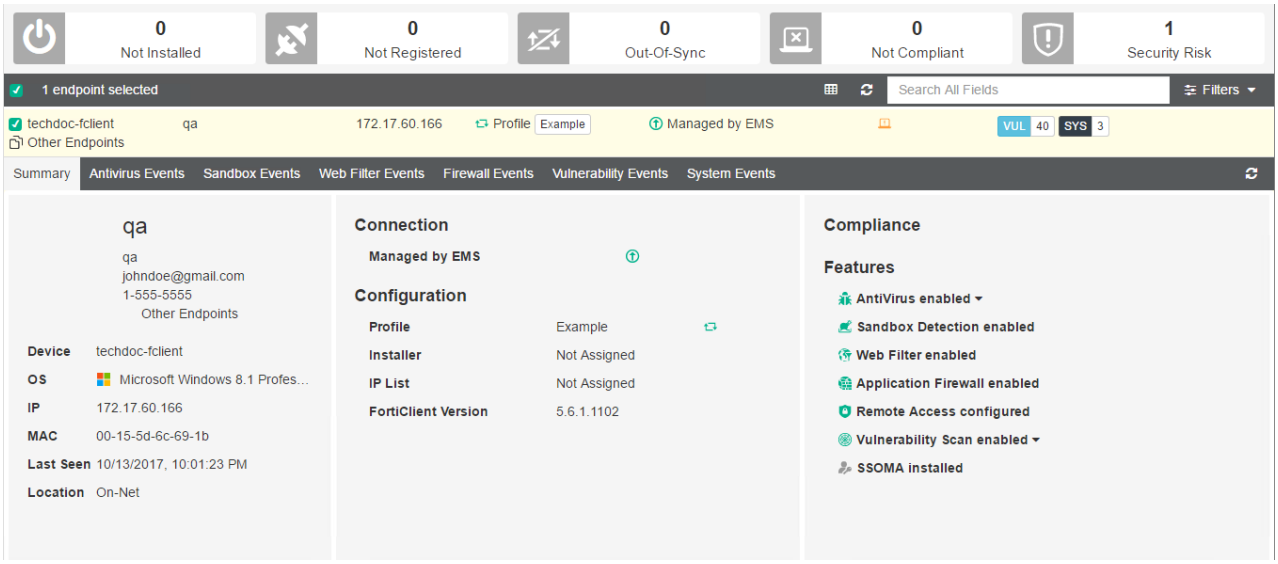
4. Click an endpoint to display its details.
5. In the *Events* column, click the *AV <number>, SB <number>, FW <number>*, *VUL<number>*, *WEB <number>* and *SYS<number>* buttons to display the associated tab of details for the selected endpont.
6. Click the *Total* button to clear the filters.
   The unfiltered list of endpoints displays.

Viewing endpoint details

You can view each endpoint's details on the *Endpoints* content pane. For a description of the options on the *Endpoints* content pane, see Viewing the Endpoints content pane on page 51.

To view endpoint details:

1. Go to *Endpoints*, and select *All Domains*, a domain, or workgroup.
   The list of endpoints for the selected domain or workgroup displays.
2. Click an endpoint to display details about it in the content pane.
   Details about the endpoint display in the content pane.



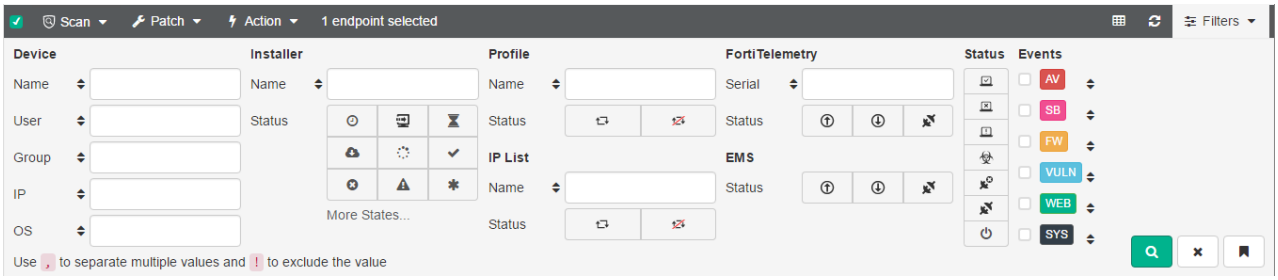
Filtering the list of endpoints

You can filter the list of endpoints displayed on the *Endpoints* content pane.

To filter endpoints:

1. Go to *Endpoints*.
2. Click *All Domains*, a domain, or workgroup.
   The list of endpoints displays.

3. Click the *Filters* menu, and set filters.
   The filter options display.
   For text values, you can use a comma (,) to separate values and an exclamation mark (!) to exclude a value.
   For buttons, hover the mouse over each button to view its tooltip.



Device		Lists the filter options for devices.
	Name	Type the name(s) to include in the filter. You can exclude a name or names from the filter using an exclamation mark (!).
	User	Type the name of the user(s) to include in the filter. You can exclude a name or names from the filter using an exclamation mark (!).
	Group	Type the name of the group(s) to include in the filter. You can also exclude a name or names from the filter using an exclamation mark (!).
	IP	Type the IP address to include in the filter. You can exclude an IP address from the filter using an exclamation mark (!).
	OS	Type the name of the operating system(s) to include in the filter. You can exclude a name or names from the filter using an exclamation mark (!).
Installer		Lists the filter options for deployment.
	Name	Type the name(s) of the installer to include in the filter. You can exclude a name or names from the filter using an exclamation mark (!).
	Status	Click one or more deployment status buttons to include in the filter. Selected status buttons are green. Hover the mouse over each button to view its tooltip. Clear the status button to exclude the status from the filter. Excluded status buttons are gray.
	More States	Click to display additional statuses to include in the filter.
Profile		
	Name	Type the name(s) of the profile to include in the filter. You can also exclude a name or names from the filter by using an exclamation mark (!).
	Status	Click the profile status to include in the filter. Selected status buttons are green. Choose between *Synced* and *Out-Of-Sync*. Clear the status button to exclude the status from the filter. Excluded status buttons are gray.

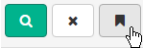
IP List		
	Name	Type the name(s) of the gateway IP list to include in the filter. You can also exclude a name or names from the filter by using an exclamation mark (!).
	Status	Click the gateway IP list status to include in the filter. Selected status buttons are green. Choose between *Synced* and *Out-Of-Sync*. Clear the status button to exclude the status from the filter. Excluded status buttons are gray.
FortiTelemetry		
	Serial	Select the FortiGate serial number to include in the filter.
	Status	Click the status for FortiClient Telemetry connection to FortiGate to include in the filter. Choose between *Online*, *Offline*, and *Not Registered*.
EMS		
	Status	Click the status for FortiClient Telemetry connection to EMS to include in the filter. Selected status buttons are green. Choose between *Online*, *Offline*, and *Not Registered*. Clear the status button to exclude the status from the filter. Excluded status buttons are gray.
Status		Click the compliance status to include in the filter. Selected status buttons are green. Choose between *Compliant*, *Not Compliant*, *Not Participating*, *Quarantined*, *Excluded*, *Not Registered*, *Not Installed*. Clear the status button to exclude the status from the filter. Excluded status buttons are gray.
Events		Select the events to include in the filter. The selected checkboxes beside the events are included in the filter. Clear the checkbox beside the event to exclude the event from the filter.
Bookmarks		Displays the list of saved filter settings. Displays only after you have saved a bookmark. Click the *Bookmark* button to name and save filter settings. Click a bookmark to use the saved settings. Click the *x* beside a bookmark to delete it.
Search		Click the *Search* button to apply the filter setting.
Reset		Click the *Reset* button to clear the filter settings.
Bookmark		Click the *Bookmark* button to save the filter settings as a bookmark.

4. Click *Search*.
   The filtered list of endpoints displays.
5. Click *Reset* to clear the filter settings.

Using bookmarks to filter the list of endpoints

You can save filter settings as bookmarks, then select the bookmarks to use them.

To create bookmarks to filter endpoints:

1. Go to *Endpoints*.
2. Click *All Endpoints*, a domain, or workgroup.
   The list of endpoints displays.
3. Click the *Filters* menu, and set filters.
4. Click the *Bookmark* button.
   
   The *New Bookmark* box displays.
5. In the *New Bookmark* box, type a name for the filter settings, and press *Enter*.
   The bookmark displays under *Bookmarks*.

To use bookmarks to filter the list of endpoints:

1. Go to *Endpoints*.
2. Click *All Endpoints*, a domain, or workgroup.
   The list of endpoints displays.
3. Click the *Filters* menu.
4. In the *Bookmarks* list, click a bookmark.
   The bookmark settings are used to filter the list of endpoints.

Managing endpoints

You can manage endpoints from the *Endpoints* pane.

Running AntiVirus scans on endpoints

You can run a full or quick AntiVirus scan on endpoints. Scanning starts on the endpoints with the next FortiClient Telemetry communication.

To run AntiVirus scans on endpoints:

1. Go to *Endpoints*.
2. Right-click a domain or workgroup, and select *Start full antivirus scan* or *Start quick antivirus scan*.

To run AntiVirus scans on an endpoint:

1. Go to *Endpoints*.
2. Select *All Endpoints*, a domain, or workgroup.

3. The list of endpoints displays in the content pane.
4. Click an endpoint, and from the *Scan* menu, select *Quick AV Scan* or *Full AV Scan*.

Running vulnerability scans on endpoints

You can run a vulnerability scan on endpoints. You can view the history of vulnerability scans for each endpoint on the *Client Details* pane.

To run vulnerability scans on endpoints:

1. Go to *Endpoints*.
2. Right-click a domain or workgroup, and select *Start vulnerability scan*.
   Vulnerability scanning starts on the endpoints with the next FortiClient Telemetry communication.

To run vulnerability scans on an endpoint:

1. Go to *Endpoints*.
2. Select *All Endpoints*, a domain, or workgroup.
   The list of endpoints displays in the content pane.
3. Click an endpoint, and from the *Scan* menu, select *Vulnerability Scan*.
   Vulnerability scanning starts on the endpoint with the next FortiClient Telemetry communication.

Patching vulnerabilities on endpoints

You can request FortiClient patch detected critical and high vulnerabilities on endpoints.

FortiClient can automatically patch many software. However, the endpoint user must manually patch some detected software vulnerabilities. If a vulnerability requires the endpoint user to download and install software to patch a vulnerability, FortiClient Console displays the information.

To patch vulnerabilities on endpoints:

1. Go to *Endpoints*.
2. Right-click a domain or workgroup, and select *Patch critical/high vulnerabilities*.
   FortiClient initiates automatic vulnerability patching with the next FortiClient Telemetry communication.

To patch vulnerabilities on an endpoint:

1. Go to *Endpoints*.
2. Select *All Endpoints*, a domain, or workgroup.
   The list of endpoints displays in the content pane.
3. Click an endpoint, and from the *Patch* menu, select one of the following options:
   - *Selected Vulnerabilities on Selected Clients*
   - *Selected Vulnerabilities on All Affected Clients*
   - *All Critical and High Vulnerabilities*

   FortiClient initiates automatic vulnerability patching with the next FortiClient Telemetry communication.

Uploading FortiClient logs

You can upload a FortiClient log file from one or several endpoints to FortiClient EMS. The log file is uploaded to the hard drive on the computer on which you are running EMS. The uploaded log file is not visible in the FortiClient EMS GUI.

To upload FortiClient logs:

1. Go to *Endpoints*.
2. Select *All Endpoints*, a domain, or workgroup.
   The list of endpoints displays in the content pane.
3. Click one or multiple endpoints, and from the *Action* menu, select *Upload FortiClient logs*.
   The `<number>_log` file is uploaded to the following location on your computer: `<drive>\Program Files (x86)\Fortinet\FortiClientEMS\logs`

Running the FortiClient diagnostic tool

You can use EMS to run the FortiClient Diagnostic Tool on one or multiple endpoints and export the results to the hard drive on the computer on which you are running FortiClient EMS. The exported information is not visible in the FortiClient EMS GUI.

To run the FortiClient diagnostic tool:

1. Go to *Endpoints*.
2. Select *All Endpoints*, a domain, or workgroup.
   The list of endpoints displays in the content pane.
3. Click one or multiple endpoints, and from the *Action* menu, select *Request Diagnostic Results*.
   The `<number>_Diagnostic_Result` file is uploaded to the following location on your computer: `<drive>:\Program Files (x86)\Fortinet\FortiClientEMS\logs`.

Updating signatures

You can use EMS to request FortiClient update signatures on the endpoints.

To update signatures:

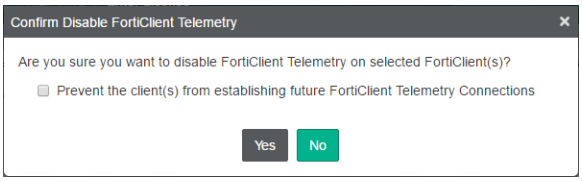
1. Go to *Endpoints*.
2. Select *All Endpoints*, a domain, or workgroup.
   The list of endpoints displays in the content pane.
3. Click an endpoint, and from the *Action* menu, select *Update Signatures*.
   FortiClient receives the request to update signatures and downloads the signatures from the Internet.

Deregistering and registering endpoints

You can manually deregister and register endpoints using EMS.

To deregister endpoints:

1. Go to *Endpoints*.
2. Click *All Endpoints*, a domain, or workgroup. A list of endpoints displays.
3. Click an endpoint, and from the *Action* menu, select *Deregister*.
   A confirmation dialog box displays.



   You can prevent the endpoint from registering in the future by selecting the *Prevent the client(s) from establishing future FortiClient Telemetry Connections* checkbox.
4. Click *Yes* to confirm.
   The endpoint is unregistered with the next FortiClient Telemetry communication.

To register endpoints:

1. Go to *Endpoints*.
2. Click *All Endpoints*, a domain, or workgroup. A list of endpoints displays.
3. Click an endpoint, and from the *Action* menu, select *Register*.
   The endpoint is registered with the next FortiClient Telemetry communication.

Quarantining endpoints

You can quarantine an endpoint using EMS. Quarantined endpoints cannot access the network.

To quarantine an endpoint:

1. Go to *Endpoints*.
2. Click *All Endpoints*, a domain, or workgroup. A list of endpoints displays.
3. Click an endpoint, and from the *Action* menu, select *Quarantine*.
   The endpoint status changes to *Quarantined*, and the endpoint is quarantined with the next FortiClient Telemetry communication.
   You can remove an endpoint from quarantine by right-clicking the endpoint and selecting *Unquarantine*. The endpoint is removed from quarantine with the next FortiClient Telemetry communication and network access is restored.

Excluding endpoints from management

You can exclude endpoints from management.

To exclude endpoints from management:

1. Right-click a domain or workgroup.
2. Select *Exclude from management*.
   The endpoint is excluded from management.

To exclude an endpoint from management:

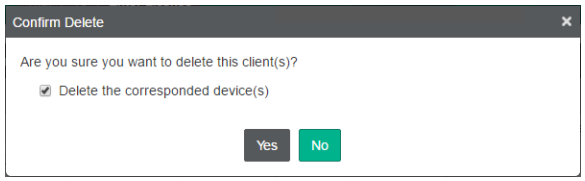
1. Go to *Endpoints*.
2. Click *All Endpoints*, a domain, or workgroup. A list of endpoints displays.
3. Click an endpoint, and from the *Action* menu, select *Exclude from Management*.
   The endpoint is excluded from management.

Deleting endpoints

You can delete unregistered endpoints from EMS.

To delete endpoints:

1. Go to *Endpoints*.
2. Click *All Endpoints*, a domain, or workgroup. A list of endpoints displays.
3. If the endpoint has a status of *Registered*, deregister the endpoint.
4. Click an endpoint, and from the *Action* menu, select *Delete Device*.
   A confirmation dialog box displays.



5. Click *Yes*.
   The endpoint is deleted from FortiClient EMS.

Endpoint Profiles

You can use the default endpoint profile or create endpoint profiles for many configurations and situations.

Configuring profiles

When you install FortiClient EMS, a default profile is created. This profile is applied to any groups you create. The default profile is designed to provide effective levels of protection. To use specific features, such as application firewall, create a new profile or change the default profile.

Consider the following when creating profiles:

- Use default settings within a profile.
- Consider the endpoint's role when changing the default profile or creating new profiles.
- Create a separate group and profile for endpoints requiring long-term special configuration.
- Use FortiClient EMS for all central profile settings, and set options for within the group instead of for the endpoint itself when possible.

Editing the default profile

You can edit the default profile to add or remove settings. You can revert to default settings by clicking *Revert to Default*.

To edit the default profile:

1. Go to *Endpoint Profiles* > *Local Profiles*, and click the *Default* profile.
2. Configure the settings on the tabs. See Profile references on page 71.
3. Click *Save* to save the profile.

Creating profiles to configure FortiClient

This section describes how to create a profile that excludes any installation or uninstallation of FortiClient software on endpoints. This type of profile is used to configure FortiClient software on endpoints.

To create profiles:

1. Go to *Endpoint Profiles* > *Manage Profiles*, and click the *Add* button.
2. In the *Profile Name* box, type the profile name.
3. On the *Deployment* tab, leave *FortiClient Deployment* disabled.
4. Configure the settings on the remaining tabs. See Profile references on page 71.
5. Click *Save* to save the profile.

Creating profiles to deploy FortiClient

You must create a new profile to deploy FortiClient to endpoints. You cannot add a FortiClient installer to the default profile.

You must add FortiClient installers to FortiClient EMS before you can select the installers in a profile. See Adding FortiClient installers on page 105.

The selected FortiClient installer in a profile controls what tabs are displayed for configuration in the profile. Only the tabs for the features in the selected installer are displayed for configuration in the profile. For example, if the installer includes only the VPN feature, only the *VPN* tab is displayed for you to configure. The *System Settings* tab always displays.

You can disable a feature included in the installer, then enable the feature in the profile later. For example, if the installer includes the Web Filter and VPN features, you can disable the Web Filter feature and keep the VPN feature enabled. When FortiClient is installed on the endpoint, the Web Filter is installed, but disabled.

To create profiles for FortiClient deployment:

1. Go to *Endpoint Profiles* > *Manage Profile*, and click the *Add* button.
2. On the *Deployment* tab, enable *FortiClient Deployment*. The FortiClient deployment options display.
3. Set the following options on the *Deployment* tab:

Action		
	Assign an	Click *Installer*.
	Installer	In the *Installer* list, select a FortiClient installer. If you have not added a FortiClient installer to FortiClient EMS, see Adding FortiClient installers on page 105. The selected FortiClient installer affects what tabs display for configuration. Only tabs related to features enabled in the FortiClient installer display for configuration.
Schedule		
	Start At	Specify what time to start installing FortiClient on endpoints.

	Prompt User If a Reboot Is Needed During Installation	Enable to prompt the end user if a reboot of the endpoint is needed. Disable to reboot the endpoint without prompting the user. If no endpoint user is logged into FortiClient, the endpoint reboots without prompt.
Credentials		
	Username	Type the username to perform deployment on AD. You must enter the admin credentials for the AD in the profile. Enter the appropriate credentials in the profile to assign to the AD. The credentials allow EMS to install FortiClient on endpoints using AD. If the credentials are wrong, the installation fails, and an error displays in EMS.
	Password	Type the password to perform deployment on AD.

4. Set the options on the remaining tabs.
5. Click *Save*.

Creating profiles to uninstall FortiClient

You can configure a profile to uninstall FortiClient from endpoints. You must create a new profile for this configuration. You cannot use the default profile to uninstall FortiClient from endpoints.

To create profiles to uninstall FortiClient:

1. Go to *Endpoint Profiles* > *Manage Profiles*, and click the *Add* button.
2. On the *Deployment* tab, enable *FortiClient Deployment*. The FortiClient deployment options display.

3. Set the following options on the *Deployment* tab:

Action		
	Assign an	Click *Uninstaller*.
Schedule		
	Start At	Specify what time to start uninstalling FortiClient from endpoints.
	Prompt User If a Reboot Is Needed During Installation	Enable to prompt the end user if a reboot of the endpoint is needed. Disable to reboot the endpoint without prompting the user. If no endpoint user is logged into FortiClient, the endpoint reboots without prompt.
Credentials		
	Username	Type the username to perform deployment on AD or workgroups. If you are using an AD to uninstall FortiClient on endpoints, you must enter the admin credentials for the AD in the profile. If you are using a workgroup to uninstall FortiClient on endpoints, FortiClient must be registered to FortiClient EMS. Admin credentials are not required. When configuring the profile, know what method (AD or workgoup) is being used to uninstall FortiClient on endpoints. If using an AD, enter the appropriate credentials in the profile you will assign to the AD. The credentials allow EMS to uninstall FortiClient on endpoints by using AD. If the credentials are wrong, the uninstallation fails, and an error displays in EMS.
	Password	Type the password to perform the uninstall on AD or workgroups.

4. Click *Save*.

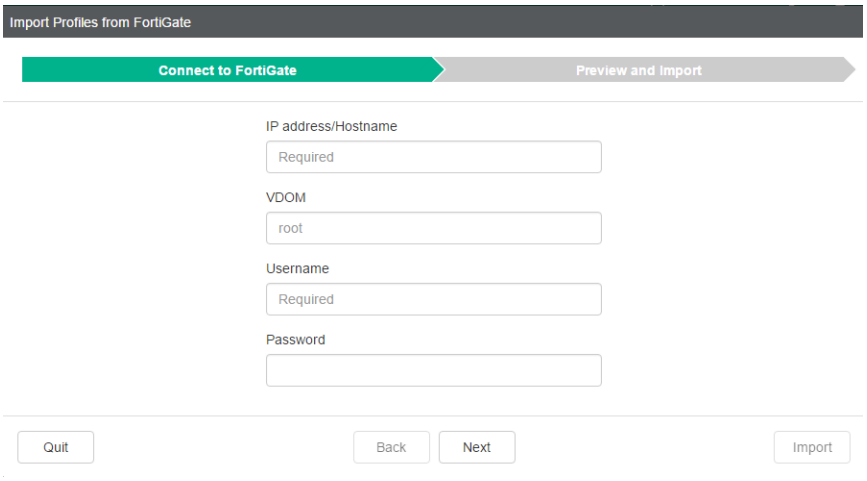
Importing FortiGate profiles

In FortiOS, endpoint profiles are called FortiClient profiles. You can import a FortiClient profile into EMS, then edit the profile in FortiClient EMS to add a FortiClient installer or add configuration information that supports the FortiGate compliance rules.

To import profiles successfully from FortiOS to FortiClient EMS, FortiGate must have the HTTPS port open. In FortiOS, go to *Network* > *Interfaces* > *Restrict Access* > *Enable checkbox for HTTPS*.

To import profiles:

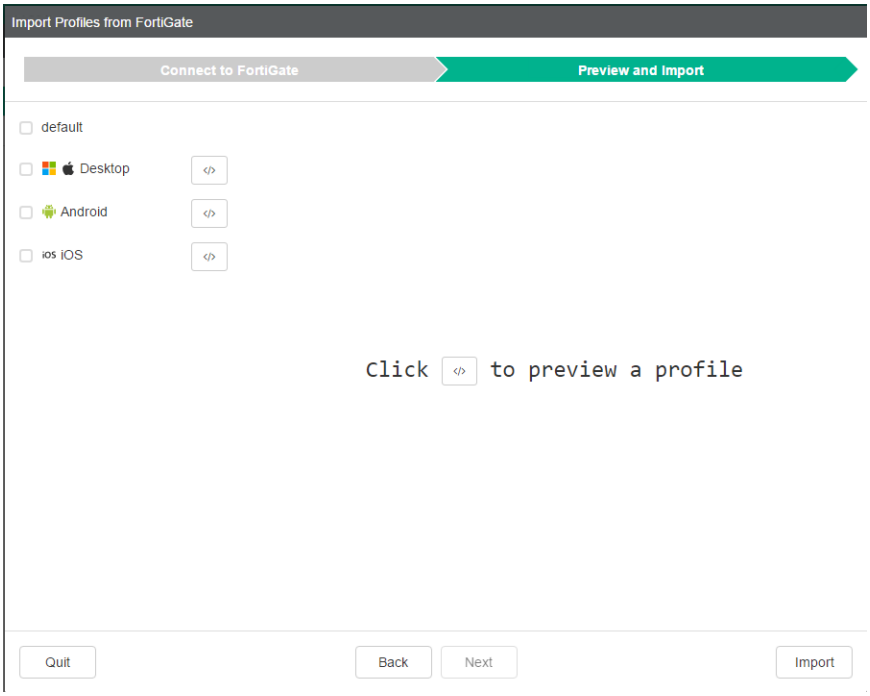
1. Click *Endpoint Profiles* > *Manage Profiles* > *Import*. The *Import Profiles from FortiGate* window opens.



2. Complete the following options, and click *Connect*.

IP address/Hostname	Enter the IP address and port of the FortiGate device from which the profile is being imported, in the format: `<ip address>:<port>`.
VDOM	Enter a VDOM name from the FortiGate if applicable.
Username	Enter the FortiGate's login username.
Password	Enter the FortiGate's login password.

The list of FortiClient profiles configured on the FortiGate displays.



Under each profile name is the list of profiles created for different operating systems, such as desktops running a Windows or Mac operating system or devices running an Android operating system. For example, under the default profile, *Desktop*, *Android* and *iOS* profiles are listed. You can click the </> icon beside each profile to preview the settings in XML format.

3. Select the profiles to import into EMS and click *Import*.

   Select the name of the profile to import all profiles for it into EMS. You can also clear the checkbox beside the profiles you do not want to import into EMS. For example, you can import the desktop and iOS profiles, but not the Android profile for a given profile name.

   The selected profiles are imported into EMS and display under the *Endpoint Profiles* pane in a group named after the FortiGate device from which they were imported.
4. In the *Endpoint Profiles* page, select an imported profile to edit it.

   The options configured in the profile by the FortiGate administrator are read-only compliance rules. You cannot change them. You can edit additional options to provide configuration information to support the compliance rules. You can also add a FortiClient installer to the profile by using the *Deployment* tab. Custom installers can be created. See Adding FortiClient installers on page 105.
5. Edit the options on the tabs.
6. Click *Save Profile*.

Creating profiles with XML

You can configure FortiClient profile settings in FortiClient EMS by using XML or a custom XML configuration file. The custom XML file must include all settings required by the endpoint at the time of deployment. For more information about how to configure a profile with XML, see the *FortiClient XML Reference* on docs.fortinet.com.

To create profiles with XML:

1. Go to *Endpoint Profiles* > *Manage Profiles*, and click the *Add* button.
2. In the *Profile Name* box, type a name for the profile.
3. Click the *Advanced* button. The *XML Configuration* tab displays, and the profile configuration displays in XML.
4. Click the *XML Configuration* tab, and click the *Edit* button.
5. Edit the XML.
6. Click *Test XML*.
7. Click *Save* to save the profile.

Creating profiles to automatically upgrade FortiClient

You can create a profile to automatically upgrade FortiClient to the latest patch release. The profile must be configured with an installer that meets the following requirements:

- The FortiClient installer was created in FortiClient EMS 1.2.0 or later.
- The FortiClient installer was created with the latest FortiClient version available for selection in FortiClient EMS at the time the installer was created.
- The FortiClient installer was created with the *Keep software updated to the latest patch release* option enabled.

See Adding FortiClient installers on page 105 for details on creating an installer.

With this configuration, when an upgrade is available, FortiClient downloads it directly from the FortiClient EMS server. Offline FortiClients remain without the upgrade until they contact the FortiClient EMS server.

To create profiles to automatically upgrade FortiClient:

1. Go to *Endpoint Profiles* > *Manage Profiles*, and click the *Add* button.
2. In the *Profile Name* box, type a name for the profile.
3. On the *Deployment* tab, enable *FortiClient Deployment*.
4. Beside *Assign an*, click *Installer*.
5. From the *Installer* dropdown list, select the desired installer, or use the *Create a New Installer* button.
6. Configure the profile as desired, then click *Save Profile*.

Viewing profiles

When you create endpoint profiles, they are listed under *Endpoint Profiles* in the left pane. You can view endpoint profiles and their settings.

To view profiles:

1. Go to *Endpoint Profiles* > *Manage Profiles*. The content pane displays the list of profiles.
2. Click a profile name, then click *Edit*. The settings display in the content pane.

Assigning profiles to endpoints

After creating the profile, you can assign the profile to domains or workgroups. When you assign the profile to domains or workgroups, the profile settings are automatically pushed to the endpoints in the domain or workgroup.

If you do not assign a profile to a specific domain or workgroup, the default profile is automatically applied.

To assign profiles:

1. Go to *Endpoints*.
2. Right-click a domain or group, select *Assign profile*, then the profile. A confirmation dialog box displays.
3. Click *Yes*. The profile is assigned.

Managing profiles

You can manage profiles from the *Endpoint Profiles* pane.

Editing profiles

When you edit a profile assigned to endpoints, the changes are automatically pushed to the endpoints when you save the profile.

To edit profiles:

1. Go to *Endpoint Profiles*, and select a profile.
2. Click *Edit*. The profile settings display in the content pane.
3. Edit the settings. See Profile references on page 71.
4. Click *Save*. If the profile is assigned to endpoints, the changes are pushed to the endpoints.

Cloning profiles

To clone profiles:

1. Go to *Endpoint Profiles* > *Manage Profiles*.
2. Select a profile, and click the *Clone* button. The cloned profile displays in the content pane.
3. In the *Profile Name* box, type a name for the profile.
4. Configure the settings on the tabs. See Profile references on page 71.
5. Click *Save*.

Deleting profiles

You cannot delete the default profile.

To delete profiles:

1. Go to *Endpoint Profiles* > *Manage Profiles*.
2. Click desired profile, then click the *Delete* button. A popup displays.
3. Click *Yes*. The profile is deleted.

Profile references

This section contains descriptions of the tabs and options used to configure profiles.

Profile Name

Option	Description
Profile Name	Type a name for the profile.

Option	Description
Basic	Select to configure the profile using the GUI.
Advanced	Select to configure the profile using XML on the *XML Configuration* tab. Displays advanced options for configuration.

AntiVirus Protection

Enable antivirus protection. Some options only display if you enable *Advanced* view. Configure the following options:

Options	Description
AntiVirus Protection	Toggle to enable or disable AntiVirus protection.
Real-Time Protection	
Scan Files as They Are Downloaded or Copied to My System	Scan files for threats as they are downloaded or copied to the system.
On Virus Discovery	• Clean Infected Files (Quarantine If Cannot Clean). This option deletes the infected file. • Repair Infected Files (Quarantine If Cannot Clean). This option extracts the virus from the infected file. This option will not work with most modern viruses. • Warn the User If a Process Attempts to Access Infected Files • Quarantine Infected Files. You can use FortiClient to view, restore, or delete the quarantined file, as well as view the virus name, submit the file to FortiGuard, and view logs. • Deny Access to Infected Files • Ignore Infected Files
Alert When Viruses Are Detected	If enabled, displays the *Virus Alert* dialog when a virus is detected while attempting to download a file via a web browser. The dialog allows you to view recently detected viruses, their locations, and statuses.
Identify Malware and Exploits Using Signatures Received from FortiSandbox	If enabled, uses signatures from FortiSandbox to identify malware and exploits. This option is available only if the *Sandbox Detection* tab is enabled. Enter the number of minutes after which to update signatures.
Block Known Communication Channels Used by Attackers	Enable to block known communication channels used by attackers.
Block All Access to Malicious Websites	Block all access to malicious websites. You must select *FortiProxy (Disable Only When Troubleshooting)* on the *System Settings* tab before you can enable this option.

Options		Description
	Use the Exclusion List Defined in the Web Filter Profile	If this option is enabled, the exclusion list on the *Web Filter* tab is used. If this option is not enabled, you must define exclusions under *Exclusions*.
Scan Compressed Files		Enable to scan compressed files for threats.
	Max Size	Configure the maximum size (in MB) of compressed files to scan. To allow scanning compressed files of any size, enter 0.
	User Process Scanning	Enable user process scanning. Select one of the following: • Scan Files When Processes Read or Write Them • Scan Files When Processes Read Them • Scan Files When Processes Write Them
Scan Network Files		Enable to scan network files for threats.
System Process Scanning		Enable system process scanning. Select one of the following: • Scan Files When System Processes Read or Write Them • Scan Files When System Processes Read Them • Scan Files When System Processes Write Them • Do Not Scan Files When System Processes Read or Write Them
On Demand Scanning		
On Virus Discovery		Select one of the following from the dropdown list: • Clean Infected Files (Quarantine If Cannot Clean). This option deletes the infected file. • Repair Infected Files (Quarantine If Cannot Clean). This option extracts the virus from the infected file. This option will not work with most modern viruses. • Warn the User If a Process Attempts to Access Infected Files • Quarantine Infected Files. You can use FortiClient to view, restore, or delete the quarantined file, as well as view the virus name, submit the file to FortiGuard, and view logs. • Ignore Infected Files
Integrate FortiClient into Windows Explorer's Context Menu		Adds a *Scan with FortiClient AntiVirus* option to the Windows Explorer right-click menu.
Pause Scanning When Running on Battery Power		Enable to pause scanning when the computer is running on battery power.
Automatically Submit Suspicious Files to FortiGuard for Analysis		Enable to automatically submit suspicious files to FortiGuard for analysis. You do not receive feedback for files submitted for analysis. The FortiGuard team is able to create signatures for any files that are submitted for analysis and determined to be malicious.

Options		Description
Scan Compressed Files		Enable to scan compressed files for threats.
	Max Size	Configure the maximum size of compressed files to be scanned in MB. To allow compressed files of any size, enter 0.
	Max Scan Speed on Computers With	Select the minimum amount of memory that must be installed on a computer to maximize scan speed: • 4 GB • 6 GB • 8 GB • 12 GB • 16 GB
Scheduled Scan		Enable scheduled scans.
Schedule Type		Select *Daily*, *Weekly*, or *Monthly*.
Scan On		If *Weekly* is selected, select the day of the week to perform the scan. If *Monthly* is selected, select the day of the month to perform the scan. Note that if you configure monthly scans to occur on the 31st of each month, the scan occurs on the first day of the month for months with fewer than 31 days.
Start At		Configure the start time for the scheduled scan.
Scan Type		Select *Quick*, *Full*, or *Custom*.
	Quick	Runs the rootkit detection engine to detect and remove rootkits. The quick scan only scans the following items for threats: executable files, DLLs, and drivers that are currently running.
	Full	Runs the rootkit detection engine to detect and remove rootkits, then performs a full system scan of all files, executable files, DLLs, and drivers. If *Full* is selected, you have the following options: • Scan removable media, if present • Scan network drives
	Custom	Runs the rootkit detection engine to detect and remove rootkits. In the *Folder* field, enter the full path of the folder on your local hard disk drive that will be scanned.
Scan Priority		Set to *Low*, *Normal*, or *High*. This refers to the amount of processing power the scan uses and its impact on other processes.
Scan Removable Media		Enable to scan connected removable media, such as USB drives, for threats.
Scan Network Drives		Enable to scan network drives for threats.

Options	Description
Enable Scheduled Scans Even When a Third-Party AV Product Is Present	Enable scheduled scans even when a third party AV product is present.
Exclusions	Enable exclusions from antivirus scanning. FortiClient EMS supports using wildcards and path variables to specify files and folders to exclude from scanning. The following wildcards and variables are supported, among others: • Using wildcards to exclude a range of file names with a specified extension, such as Edb*.jrs • Using wildcards to exclude all files with a specified extension, such as *.jrs • Path variable %windir% • Path variable %allusersprofile% • Path variable %systemroot% • Path variable %systemdrive% Note that having a longer exclusion list affects antivirus performance. It is advised to keep the exclusion list as short as possible.
Paths to Excluded Folders	Enter fully qualified excluded folder paths in the provided text box to exclude these folders from antivirus scanning.
Paths to Excluded Files	Enter fully qualified excluded files in the provided text box to exclude these files from antivirus scanning.
File Extensions Excluded from Real-Time Protection	Enter file extensions to exclude from realtime AV protection.
File Extensions Excluded from On Demand Scanning	Enter file extensions to exclude from on demand AV protection.
Other	
Scan for Rootkits	Enable to scan for rootkits. A rootkit is a collection of programs that enable administrator-level access to a computer or computer network. Typically a rootkit is installed on a computer after first obtaining user-level access by exploiting a known vulnerability or cracking a password.
Scan for Adware	Enable to scan for adware. Adware is a form of software that downloads or displays unwanted ads when a user is online.
Scan for Riskware	Enable to scan for riskware. Riskware refers to legitimate programs which, when installed and executed, presents a possible but not definite risk to the computer.

Options	Description
Enable Advanced Heuristics	Enable advanced heuristics. Advanced heuristics is a sequence of heuristics to detect complex malware.
Scan Removable Media on Insertion	Enable to scan removable media (CDs, DVDs, Blu-ray disks, USB keys etc.) on insertion.
Scan Email	Enable to scan emails for threats.
Scan MIME files (Inbox Files)	Enable to scan MIME files. Multipurpose Internet Mail Extensions (MIME) is an Internet standard that extends the format of the email to support the following: • Text in character sets other than ASCII • Non text attachments (audio, video, images, applications) • Message bodies with multiple parts
Enable FortiGuard Analytics	Automatically sends suspicious files to FortiGuard for analysis.
Notify Logged in Users if Their AV Signatures Expired	Enable to notify logged in users if their AntiVirus signatures have expired.

Sandbox Detection

Enable Sandbox Detection. Some options only display if you enable *Advanced* view. Configure the following options:

Options		Description
Sandbox Detection		Enable or disable Sandbox Detection.
Server		
	IP Address/Hostname	Enter the IP address/host name of the FortiSandbox unit. If the endpoint has not been authorized to connect to the specified FortiSandbox unit, a *Not Authorized* icon displays beside this field.
	Wait for FortiSandbox Results before Allowing File Access	Enable to have the endpoint user wait for FortiSandbox scanning results before being allowed access to files. Set the timeout in seconds. Disable to allow the endpoint user to access files before FortiSandbox results are provided.
	Deny Access to File If FortiSandbox Is Unreachable	You have the option to: • Deny Access to Downloaded Files If FortiSandbox Is Offline. • Enter the *Timeout* value in seconds. File access is allowed if FortiSandbox results are not received when the timeout expires. Set to `-1` to infinitely restrict access to the file.
Submission		

Options		Description
	All Files Executed from Removable Media	Select to submit all files executed on removable media, such as USB drives, to FortiSandbox for analysis.
	All Files Executed from Mapped Network Drives	Enable to submit all files executed from mapped network drives.
	All Web Downloads	Enable to submit all web downloads.
	All Email Downloads	Enable to submit all email downloads.
Remediation		
	Action	Choose *Quarantine* or *Alert & Notify* for infected files.
Exceptions		
	Exclude Files from Trusted Sources	Enable to exclude files from trusted sources.
	Exclude Specified Folders/Files	Enable to exclude specified folders/files. You must also create the exclusion list.

Web Filter

You must enable *FortiProxy (Disable Only When Troubleshooting)* on the *System Settings* tab to use the *Web Filter* options.

Configuration		Description
Web Filter		Enable or disable web filtering.
General		
	Client Web Filtering When On-Net	Enable client web filtering when on-net.
	Log All URLs	Enable to log all URLs.
	Log User Initiated Traffic	Enable to log user initiated traffic.
Site Categories		Select to enable site categories. When site categories are disabled, FortiClient is protected by the exclusion list. See the FortiGuard website for descriptions of the available categories and subcategories.

Configuration		Description
	Adult/Mature Content	Select one of the following: • Block • Warn • Allow • Monitor
	Bandwidth Consuming	Select one of the following: • Block • Warn • Allow • Monitor
	General Interest-Business	Select one of the following: • Block • Warn • Allow • Monitor
	General Interest-Personal	Select one of the following: • Block • Warn • Allow • Monitor
	Potentially Liable	Select one of the following: • Block • Warn • Allow • Monitor
	Security Risk	Select one of the following: • Block • Warn • Allow • Monitor
	Unrated	Select one of the following: • Block • Warn • Allow • Monitor
	Rate IP Addresses	Enable to rate all IP addresses.

Configuration	Description
Exclusion List	
Action	Select one of the following actions: • Allow • Block • Monitor
URL	Enter specific URLs to allow, block, or monitor.
Type	Select one of the following types: • Simple • Wildcard • Regular Expression Wildcard characters and Perl Compatible Regular Expressions (PCRE) can be used.

Application Firewall

Configuration	Description
Application Firewall	Enable or disable application control.
Notification Bubbles on User's Desktop When Applications Are Blocked	Enable notification bubbles when applications are blocked.
Detect & Block Exploits	Enable to detect and block exploits.

Configuration	Description
Categories	Block, allow or monitor the following categories: 1. Botnet 2. Business 3. Cloud.IT 4. Collaboration 5. Email 6. Game 7. General.Interest 8. Industrial 9. Mobile 10. Network.Service 11. P2P 12. Proxy 13. Remote.Access 14. Social.Media 15. Storage.Backup 16. Update 17. Video/Audio 18. VoIP 19. Web.Client 20. All Other Known Applications 21. All Other Unknown Applications
Application Overrides	
Delete	Delete an application.
Add Signature	Add a signature to an application.

VPN

Configuration		Description
VPN		Enable or disable VPN use.
General		
	Allow Personal VPN	Enable to allow personal VPN.
	Disable Connect/Disconnect	Enable to disable connect/disconnect.
	Show VPN before Logon	Enable to show VPN before logon.

Configuration		Description
	Use Windows Credentials	Use Windows credentials for VPN.
	Minimize Window on Connect	Enable to minimize the window upon connecting.
	Show Negotiation Window	Enable to show negotiation window.
	Use Vendor ID	Enable to use vendor ID. Enter the vendor ID in the Vendor ID box.
	Current Connection	Select the current VPN tunnel.
	Keep Running Max Tries	Enter the maximum number of attempts. It cannot be a negative value.
SSL VPN		Enable SSL VPN.
	DNS Cache Service Control	FortiClient disables Windows OS DNS cache when an SSL VPN tunnel is established. The DNS cache is restored after SSL VPN tunnel is disconnected. If it is observed that FSSO clients do not function correctly when an SSL VPN tunnel is up, use the following XML configuration to control DNS cache.
	Prefer SSL VPN DNS	When disabled, custom DNS server from SSL VPN will not be added to physical interface. When enabled, custom DNS server from SSL VPN will be prepended to physical interface.
IPSec VPN		Enable IPSec VPN.
		Enable or disable the following: 1. Beep if Error 2. Use Windows Store Certificates 3. Current User Windows Store Certificates (IPsec only) 4. Local Computer Windows Store Certificates (IPSec only) 5. Use Smart Card Certificates 6. Show Auth Certificates Only 7. Block IPv6 8. Enable UDP Checksum 9. Disable Default Route 10. Check for Certificate Private Key 11. Enhanced Key Usage Mandatory

The following options are available in the *Creating VPN Tunnel* window after clicking the *Add Tunnel* button in the *VPN Tunnels* section.

Basic Settings

	Name	Enter a VPN name.
	Type	Select *SSL VPN* or *IPsec VPN*.
	Remote Gateway	Enter the IP address/hostname of the remote gateway. Multiple remote gateways can be configured by separating each entry with a semicolon. If one gateway is not available, the VPN will connect to the next configured gateway.
	Port	Enter the access port. Available if *SSL VPN* is selected. The default port is 443.
	Require Certificate	Enable to require a certificate. Available if *SSL VPN* is selected.
	Authentication Method	Select the authentication method for the VPN. Available if *IPsec VPN* is selected.
	Pre-Shared Key	Enter the pre-shared key required. Available if *Pre-Shared Key* is selected for *Authentication Method*.
	Prompt for Username	Enable to prompt for the username when accessing VPN.
VPN Settings		Available if *IPsec VPN* is selected for the VPN type.
	Mode	Select *Main* or *Aggressive*.
	Options	Select *Mode Config*, *Manual Set*, or *DHCP over IPsec*.
	Specify DNS Server (IPv4)	Specify the DNS server for the VPN tunnel. Available if *Manual Set* is selected.
	Assign IP Address (IPv4)	Enter the IP address to assign for the VPN tunnel. Available if *Manual Set* is selected.
	Split Table	Enter the IP address and subnet mask for the VPN tunnel. Available if *Manual Set* or *DHCP over IPsec* is selected.
Phase 1		Available if *IPsec VPN* is selected for the VPN type. Select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required. You need to select a minimum of one and a maximum of two combinations. The remote peer or client must be configured to use at least one of the proposals that you define.
	Encryption	Select the encryption standard.
	Authentication	Select the authentication method.

	DH Groups	Select one or more Diffie-Hellman groups from DH group 1, 2, 5, 14, 15, 16, 17, 18, 19 and 20. At least one of the DH Group settings on the remote peer or client must match one the selections on the FortiGate unit. Failure to match one or more DH groups will result in failed negotiations.
	Key Life	Enter the time (in seconds) that must pass before the IKE encryption key expires. When the key expires, a new key is generated without interrupting service. The key life can be from 120 to 172,800 seconds.
	Local ID	Enter the local ID.
	Enable Implied SPDO	Enable implied SPDO. Enter the timeout in seconds.
	Dead Peer Detection	Select this checkbox to reestablish VPN tunnels on idle connections and clean up dead IKE peers if required.
	NAT Traversal	Select the checkbox if a NAT device exists between the client and the local FortiGate unit. The client and the local FortiGate unit must have the same NAT traversal setting (both selected or both cleared) to connect reliably.
	Enable Local LAN	Enable local LAN.
	Enable IKE Fragmentation	Enable IKE fragmentation.
Phase 2		Available if *IPsec VPN* is selected for the VPN type. Select the encryption and authentication algorithms that will be proposed to the remote VPN peer. You can specify up to two proposals. To establish a VPN connection, at least one of the proposals that you specify must match configuration on the remote peer.
	Encryption	Select the encryption standard.
	Authentication	Select the authentication method.
	DH Group	Select one Diffie-Hellman (DH) group (1, 2, 5, 14, 15, 16, 17, 18, 19 or 20). This must match the DH Group that the remote peer or dialup client uses.
	Key Life	The Key Life setting sets a limit on the length of time that a phase 2 key can be used. The default units are seconds. Alternatively, you can set a limit on the number of kilobytes (KB) of processed data, or both. If you select both, the key expires when either the time has passed or the number of KB have been processed. When the phase 2 key expires, a new key is generated without interrupting service.

	Enable Replay Detection	Replay detection enables the unit to check all IPsec packets to see if they have been received before. If any encrypted packets arrive out of order, the unit discards them.
	Enable Perfect Forward Secrecy (PFS)	Select the checkbox to enable Perfect forward secrecy (PFS). PFS forces a new Diffie-Hellman exchange when the tunnel starts and whenever the phase 2 key life expires, causing a new key to be generated each time.
	Auto Keep Alive	Enable auto keep alive.
Advanced Settings		
	Enable One-Time Password	Enable one-time password.
	Enable XAuth	Enable XAuth.
	Enable Single User Mode	Enable Single User Mode.
	Show Passcode	Enable to remember your password.
	Save Username	Enable to save your username.
	Show "Remember Password" Option	Enable to have the VPN tunnel remember the password.
	Show "Always Up" Option	Enable to have the VPN tunnel always up. This also needs to be enabled on the FortiGate.
	Show "Auto Connect" Option	Enable to automatically connect the VPN tunnel. This also needs to be enabled on the FortiGate.
	On Connect Script	Enable the on connect script. Enter your script. This also needs to be enabled on the FortiGate.
	On Disconnect Script	Enable the disconnect script. Enter your script. This also needs to be enabled on the FortiGate.

Vulnerability Scan

Configuration	Description
Vulnerability Scan	Enable or disable Vulnerability Scan.
Scan on Registration	Scan endpoints upon connecting to a FortiGate.
Scan on Signature Update	Scan endpoints upon updating a signature.
Scan for OS Updates	Scan for OS updates.
Scheduled Scan	Configure settings for scheduled scanning.

Configuration		Description
	Schedule Type	Configure either *Daily*, *Weekly*, *Monthly*.
	Scan On	Configure the day the scan will run (1st-31st of the month). This only applies if the schedule type is configured to *Monthly*.
	Start At	Configure the time the scan will start.
Automatic Patching		
	Patch Level	When enabled, patches are installed automatically when vulnerabilities are detected. Select one of the following: • Critical: Patch critical vulnerabilities only • High: Patch high severity, and above, vulnerabilities • Medium: Patch medium severity, and above, vulnerabilities • Low: Patch low severity, and above, vulnerabilities • All: Patch all vulnerabilities. Automatic patching may require endpoint reboot.
Exclusions		
	Exempt Application Vulnerabilities Requiring Manual Update from Vulnerability Compliance Check	When enabled, all applications that require the endpoint user to manually patch vulnerabilities are excluded from vulnerability scanning.
	Exclude Selected Applications from Vulnerability Compliance Check	In the *<number> Applications* list, click the applications to exclude, and they are automatically moved to the *<number> Excluded Applications* list. In the *<number> Excluded Applications* list, click the applications to remove from the exclusion list.
	Disable Automatic Patching for These Applications	Disable automatic patching for the applications excluded from vulnerability compliance check.

System Settings

Configuration	Description
UI	Specify how the FortiClient user interface appears when installed on endpoints.
Show Dashboard Banner	Enable the dashboard banner.
Password Lock Configuration	Turn on the password lock for FortiClient.

Configuration	Description
Password	Type a password.
Do Not Allow User to Back Up Configuration	Enable to not allow users to back up configuration.
Hide System Tray Icon	Enable to hide the system tray icon.
Culture Code	Configure the culture code. Select one of the following: • os-default • zh-tw • cs-cz • de-de • en-us • fr-fr • hu-hu • ru-ru • ja-jp • ko-kr • pt-br • sk-sk • es-es • zh-cn • et-ee • lv-lv • lt-lt • fi-fi • sv-se • da-dk • pl-pl • nb-no
Log	Specify FortiClient log settings.
Level	Click *Advanced*, and select one of the following: • Emergency: The system becomes unstable. • Alert: Immediate action is required. • Critical: Functionality is affected. • Error: An error condition exists and functionality could be affected. • Warning: Functionality could be affected. • Notice: Information about normal events. • Info: General information about system operations. • Debug: Debug FortiClient.

Configuration		Description
Features		Enable any or all of the following: • AntiVirus • Application Firewall • Telemetry • FSSOMA • Proxy • IPsec VPN • SSL VPN • Update • Vulnerability • Web Filter • Sandbox
Client-Based Logging When On-Net		Turn on client-based logging when onnet. For information about the onnet feature, see the *FortiClient Administration Guide*.
Upload Logs to FortiAnalyzer/FortiManager		Turn on to upload FortiClient logs to the FortiAnalyzer or FortiManager device at the specified address or hostname.
	Upload Traffic Logs	Enable to upload traffic logs.
	Upload Vulnerability Logs	Enable to upload vulnerability logs.
	Upload Event Logs	Enable to upload event logs.
	IP Address/Hostname	Enter the IP address. When connecting to FortiAnalyzer 5.6+, use the format *https://FAZ-IP:port/logging*. Otherwise, use the format *https://FAZ-IP/jsonrpc/fazapi/logs*.
	SSL Enabled	Enable SSL.
	Upload Schedule (minutes)	Configure the upload schedule in minutes.
	Log Generation Timeout (seconds)	Configure the log generation timeout in seconds.
	Log Retention (days)	Configure the duration of time to retain logs in days.
Proxy		
Use Proxy for Updates		Enable to use proxy for updates.
	Connect to FDN Directly If Proxy Is Offline	Enable to connect to FDN directly if proxy is offline.

Configuration		Description
Use Proxy for Virus Submission		Enable to use proxy for virus submission.
	Type	Configure the type. Options include: • http • socks4 • socks5
	IP Address/Hostname	Enter IP address/hostname.
	Port	Enter the port number.
	Username	Enter the username.
	Password	Enter the password. Enable Show Password to show the password in plain text.
Update		Specify whether to use FortiManager to update FortiClient on endpoints
Use FortiManager for Client Software/Signature Update		Turn on to enable FortiClient EMS to obtain antivirus signatures and software updates from the FortiManager device at the specified IP address or hostname.
	IP Address/Hostname	Enter the IP address/hostname.
	Port	Enter the port number.
	Failover Port	Enter the failover port.
	Timeout	Enter the timeout interval.
	Failover to FDN When FortiManager Is Not Available	Enable failover to FDN when FortiManager is not available.
Auto Patch		Enable auto patch.
	Update Action	Select one of the following: • Notify Only The Update Action will be set to *Disabled*. The Advanced XML configuration should be: `<update_action>disable</update_action>` • Download And Install • Download Only
Scheduled Updates		Enable to configure the update schedule.
	Schedule Type	Select *Interval* or *Daily* for your schedule time.

Configuration		Description
	Update Every	Configure the interval.
FortiProxy		Enable FortiProxy (disable only when troubleshooting). You must enable FortiProxy to use the Web Filter options as well as some AntiVirus options.
HTTPS Proxy		Enable HTTPS proxy.
	HTTP Timeout	Enter the HTTP timeout interval.
POP3 Client Comforting		Enable POP3 client comforting.
POP3 Server Comforting		Enable POP3 server comforting.
SMTP Client Comforting		Enable SMTP.
Self Test		Enable Self Test. You have the option to *Notify* the *Last Port*.
	Notify	Enable Notify and enter the last port.
	Last Port	Last port number.
Endpoint Control		Specify settings for the endpoints.
Show Bubble Notifications		Enable to show bubble notifications.
Show Profile Details		Enable to show profile details.
Silent Registration		Turn on to enable silent registration of endpoints, which means that endpoints are registered without user interaction. Turn off to require user interaction to register endpoints.
Log off When User Logs Out of Windows		Turn on to log off FortiClient when the endpoint user logs out of Windows. Turn off to remain logged in.
Disable Unregister		Turn on to forbid users from unregistering FortiClient from FortiClient EMS. Turn off to allow users to unregister FortiClient from FortiClient EMS.
	Disable FortiGate Switch	Enable to disable FortiGate switch.
Hide Compliance Enforcement Feature Message from Compliance Tab		Enable to hide the compliance encoforcement feature message from the *Compliance* tab. This option is only enforced on FortiClients registered to FortiClient EMS. This option does not apply to monitored clients.
On-Net Subnets		Turn on to enable onnet subnets.
	IP Addresses/Subnet Masks	Enter IP addresses/subnet mask to connect to onnet subnets.

Configuration		Description
Gateway MAC Address		Enable gateway MAC address.
	MAC Addresses	Enter MAC addresses.
Other		
Install CA Certificate on Client		Turn on to select and install a CA certificate on the FortiClient endpoint. You can add certificates by going to *Administration* > *CA Certificate Management*.
FortiClient Single Sign-On Mobility Agent		Select to enable Single Sign-On Mobility Agent for FortiAuthenticator. To use this feature you need to apply a FortiClient SSO mobility agent license to your FortiAuthenticator device.
	IP Address/Hostname	Enter the FortiAuthenticator IP address or hostname.
	Port	Enter the port number.
	Pre-Shared Key	Enter the pre-shared key. The pre-shared key should match the key configured on your FortiAuthenticator device.
WAN Optimization		Enable WAN optimization.
	Maximum Disk Cache Size	Select either *512* or *1024* MB.
iOS		
Distribute Configuration Profile (.mobileconfig file)		Enable and browse for your `.mobileconfig` file to distribute the configuration profile.
Privacy		
	Send Usage Statistics to Fortinet	Fortinet uses sent usage statistics to improve product quality and user experience.

XML Configuration

Configuration	Description
XML editor	Configure using the XML editor. See the FortiClient XML Reference Guide in the Fortinet Document Library.

Gateway IP Lists

Gateway IP lists are useful when using FortiClient EMS integrated with FortiGate. If using FortiClient EMS without FortiGate, you are not required to use gateway IP lists.

You can use gateway IP lists to specify what IP addresses or fully qualified domain names (FQDN) and ports endpoints can use to connect FortiClient Telemetry to FortiGate, EMS, or FortiGate and EMS. You can create one or more gateway IP lists and assign them to domains or workgroups.

After deploying FortiClient to endpoints, FortiClient uses the gateway IP list to try and connect FortiClient Telemetry to FortiGate or EMS. This connection is based on the gateway IP list received from EMS.

Even if the endpoint is already connected to a FortiGate, you can still assign a gateway IP list to endpoints. You can also update existing gateway IP lists as required. The updates are pushed to endpoints with the next Telemetry communication.

Creating gateway IP lists

Gateway IP lists are useful when using FortiClient EMS integrated with FortiGate. If using FortiClient EMS without FortiGate, you are not required to use gateway IP lists.

You can create one or more gateway IP lists. Each list can contain IP addresses for multiple FortiGate units.

To create gateway IP lists:

1. Go to *Gateway IP Lists* > *Manage Gateway Lists*.
2. Click the *Add* button.

3. Configure the following:

Name		Enter the list name.
Comment		Enter additional comments (optional).
IP addresses/hostnames		Enter the IP address and port for FortiGate devices using the following format: IP:port. You can also use an FQDN. Press the *Enter* key to add additional IP addresses.
Connect to local subnets only		Enable to only allow to connect to local subnets.
Use connection key		Enable the connection key endpoints can use to connect to FortiGate units.
	New connection key	Enter the connection key.
	Confirm new connection key	Reenter the connection key to confirm.
Monitored by EMS		Select an option from the dropdown list. Users can configure this IP address in *System Settings* > *Server*.

4. Click *Save*.

Exporting gateway IP lists to XML

After you create and save a gateway IP list, the *Export XML* button displays, and you can export the list to a configuration file in XML format.

To export Gateway IP lists to XML:

1. Go to *Gateway IP Lists* > *Manage Gateway Lists*.
2. Click a list.
3. Click the *Export* button.

   A `<filename>.conf` file is downloaded to your computer. Following is an example of the XML:

```
<?xml version="1.0" encoding="utf-8"?>
<forticlient_configuration>
   <endpoint_control>
      <fortigates>
         <fortigate>
            <name>FortiGate</name>
            <registration_password></registration_password>
            <addresses>1.1.1.1:8013</addresses>
         </fortigate>
      </fortigates>
      <notification_server>
         <registration_password></registration_password>
         <address>1.1.1.1:8013</address>
      </notification_server>
   </endpoint_control>
```

```
</forticlient_configuration>
```

Viewing gateway IP lists

When you create gateway IP lists, they are listed under *Gateway IP Lists* in the left pane. You can view the gateway IP lists and their settings.

To view gateway IP lists:

1. Under *Gateway IP Lists*, click the desired gateway IP list to display it in the content pane.

Assigning gateway IP lists to endpoints

After creating a gateway IP list, you can assign the list to endpoints. When you assign the IP list and FortiClient Telemetry data registration process has started, the endpoint connects to a FortiGate or EMS, based on the gateway IP list.

To assign gateway IP lists to endpoints:

1. Go to *Endpoints*.
2. Right-click a domain or workgroup, and select *Assign gateway list*.
3. Select the desired list or create a new gateway IP list.

Viewing assigned gateway IP lists

To view assigned gateway IP lists:

1. Select an endpoint.
2. View *Summary* > *Configuration* > *IP List*.

Deployment

You can use FortiClient EMS to deploy FortiClient on endpoints that are part of an Active Directory (AD) server. Deploying FortiClient from FortiClient EMS requires the following steps:

- Preparing the AD server for deployment
- Deploying FortiClient on endpoints

After FortiClient is deployed on endpoints, and endpoints are connected to FortiClient EMS, you can update endpoints by editing the associated profiles.

You can also use FortiClient EMS to uninstall and upgrade FortiClient on endpoints that are part of an AD server.

You cannot use workgroups to deploy an initial installation of FortiClient to endpoints. However, after FortiClient is installed on endpoints and endpoints connect to FortiClient EMS, you can use workgroups to uninstall and update FortiClient on endpoints.

You cannot use FortiClient EMS to deploy an initial installation of FortiClient (Mac OS X) to endpoints. However, after FortiClient (Mac OS X) is installed on endpoints and endpoints connect to FortiClient EMS, you can use FortiClient EMS to uninstall and update FortiClient (Mac OS X) on endpoints.

Preparing the AD server for deployment

Before you can successfully deploy a FortiClient installation, ensure you install and prepare the AD server as follows:

- Configure a group policy on the AD server.
- Configure the required Windows services on the AD server.
- Create deployment rules for Windows firewall.
- Configure Windows firewall domain profile settings.

Configuring a group policy on the AD server

To configure a group policy on the AD server:

1. On the AD server, open *Group Policy Management*.
2. Right-click the *Default Domain Policy* setting. The Group Policy Management Editor opens.

   A new policy is applied to the entire AD domain. Alternatively, you can create a new Group Policy Object, and link it to one or more organizational units (OU) in the AD server that contains the endpoint computers on which FortiClient will be deployed.

Configuring required Windows services

To configure required Windows services:

1. In the Group Policy Management Editor, in the left panel, go to *Computer Configuration* > *Policies* > *Windows Settings* > *Security Settings* > *System Services*.
2. In the right panel, select the following:
   a. Task Scheduler: Automatic
   b. Windows Installer: Manual
   c. Remote Registry: Automatic

Creating deployment rules for Windows firewall

To create deployment rules for Windows firewall:

1. In the Group Policy Management Editor, in the left panel, go to *Computer Configuration* > *Policies* > *Windows Settings* > *Security Settings* > *Windows Firewall with Advanced Security* > *Inbound Rules*.
2. Right-click *Inbound Rules* and select *New Rule*.
3. Select *Predefined* from the dropdown list and select *File and Printer Sharing*.
4. Click *Next*.
5. Ensure that the *File and Printer Sharing (SMB-In)* box is selected and click *Next*.
6. Select *Allow the connection* and click *Finish*.
7. Repeat steps 1 to 2.
8. Select *Predefined* from the dropdown list and select *Remote Scheduled Tasks Management* and click *Next*.
9. Ensure that the *Remote Scheduled Tasks Management (RPC)* box is checked and click *Next*.
10. Select *Allow the connection* and click *Finish*.

Configuring Windows firewall domain profile settings

To configure Windows firewall domain profile settings:

1. In the Group Policy Management Editor, in the left panel, go to *Computer Configuration* > *Policies* > *Administrative Templates* > *Network* > *Network Connections* > *Windows Firewall* > *Domain Profile*.
2. Select *Allow inbound file and printer sharing* exception:
   a. Right-click and select *Edit*.
   b. Enable the radio button.
   c. Provide the EMS server's IP address in the text box.
   d. Allow unsolicited incoming messages from these IP addresses.
   e. Click OK.
3. Select *Allow inbound remote administration* exception.
   Repeat steps listed in step 2 above to create an exception.
4. Select *Allow ICMP Exceptions*:
   a. Right-click and select *Edit*.
   b. Enable the radio button.

c. Select the *Allow inbound echo request* checkbox.
d. Click *OK*.

To deploy the group policy manually, execute `gpupdate /force` on the AD server to update the group profile on all endpoints.
Execute `gpresult.exe /H gpresult.html` on any AD client to view the group policy deployed on the endpoints.

Preparing Windows endpoints for FortiClient deployment

The following services must be enabled and configured on each Windows endpoint before FortiClient is deployed to them:

- Task Scheduler: Automatic
- Windows Installer: Manual
- Remote Registry: Automatic

The Windows Firewall must be configured to allow the following inbound connections:

- File and Printer Sharing (SMB-In)
- Remote Scheduled Tasks Management (RPC)

For AD group deployments, an AD administrator account is required. For non-AD deployments, the installer URL can be shared with users, who can then download and install FortiClient manually. You can locate the installer URL in *Software Management*. Go to *Administration* > *Software Management*.

Deploying FortiClient on endpoints

Before you can successfully deploy a FortiClient installation from FortiClient EMS using an AD server, you must have prepared the AD server. See Preparing the AD server for deployment on page 94.

To deploy FortiClient by using AD servers

1. Add the AD server to FortiClient EMS by adding a domain. See Adding endpoints using an Active Directory domain server on page 50.
2. Add a FortiClient installer package to FortiClient EMS. See Adding FortiClient installers on page 105.
3. Add a profile, select the FortiClient installer package, and configure FortiClient features in the profile. See Creating profiles to deploy FortiClient on page 65.
4. Assign the profile to a branch of the AD domain to push the FortiClient installation process on the endpoints. See Assigning profiles to endpoints on page 70.
5. Verify the deployment by monitoring FortiClient registrations to the FortiClient EMS.

Deploying initial installations of FortiClient (Mac OS X)

FortiClient EMS cannot be used to deploy initial installations of Forticlient (Mac OS X). You can deploy an initial installation of FortiClient (Mac OS X) by doing one of the following:

- Create a custom FortiClient (Mac OS X) installer on FortiClient EMS with the EMS IP address embedded. Send the installer download link to users so they can install FortiClient manually on the endpoint. Once installed, FortiClient (Mac OS X) automatically connects to FortiClient EMS and supports future deployments from FortiClient EMS directly. It is recommended to enable compliance on the FortiGate (set as warning) and put the installer download link so users can download it from the captive portal.
- Use a third party application to perform initial deployment of FortiClient (Mac OS X) to endpoints.

After FortiClient (Mac OS X) is installed on endpoints and has connected FortiClient Telemetry to FortiClient EMS, you can use FortiClient EMS to replace, upgrade, and uninstall FortiClient (Mac OS X).

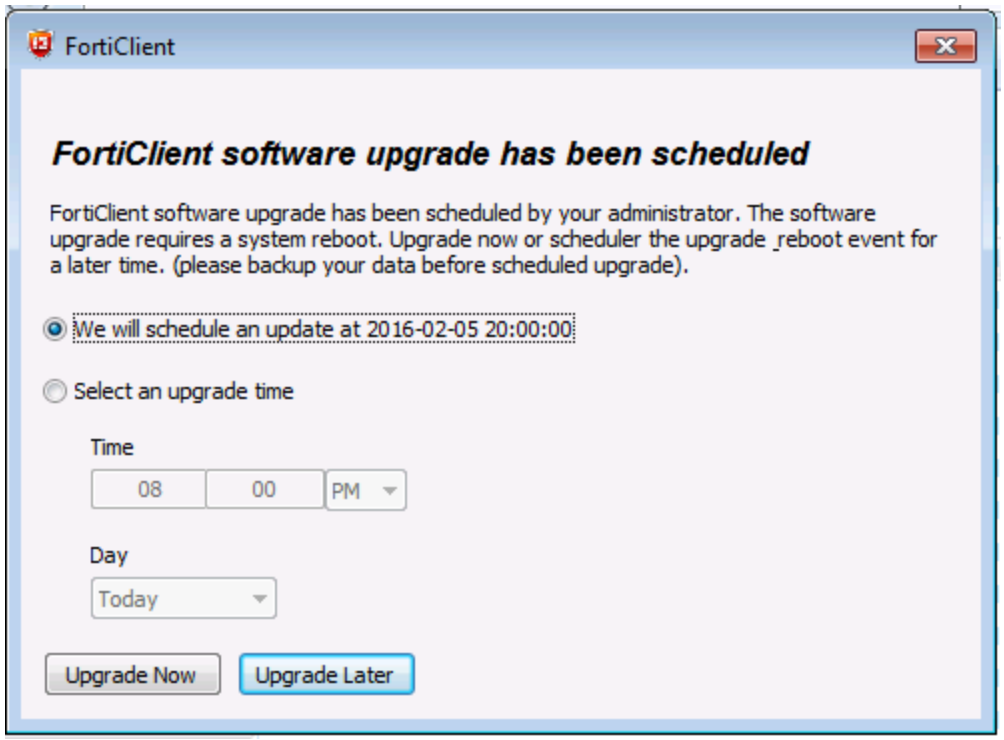
Deploying FortiClient upgrades from EMS

You can deploy a FortiClient software update from EMS. A prompt appears on the FortiClient endpoint when an installer package is requested to be deployed. The prompt requests the user to do one of the following:

1. Upgrade Now

   If this option is selected, it performs the upgrade and automatically restarts your computer.
2. Upgrade Later

   If this option is selected, you can indicate the time to start the upgrade. The default is 8:00 PM. Your computer automatically restarts after the upgrade has finished.



3. No Option

   If no option is selected, the upgrade occurs by default at 8:00 PM.

   After FortiClient EMS uninstalls the previous version, it asks if the user wants to reboot. The prompt requests the user to do one of the following:

   a. Reboot Now

      Select this option to have the reboot occur immediately.

   b. Reboot Later

      Select this option to indicate the time to reboot.

   c. Cancel Reboot

      Select this option to cancel the reboot request and reboot at your discretion.

Administration

Administrators

This section describes the default user accounts and permissions for FortiClient EMS. It also describes how to change the administrator password and configure Windows users.

Default user account and permissions

The default user named *admin* has complete access to all FortiClient EMS permissions, including modification, user permissions, approval, discovery, and deployment.

The *admin* user has access to all configured Windows and LDAP servers and users and has the authority to configure user privileges and permissions. If you are not authorized for certain tasks or devices, the related menu items, items in content pages, and buttons are hidden or disabled. In addition, a message informs you that you do not have permission to view the selected information or perform the selected operation.

Viewing users

You can view the default *admin* user and all users added to FortiClient EMS.

To view users:

1. Go to *Administration* > *Administrators*.
   The following information displays:

Add	Add a new user.
Refresh	Refresh the list of users.
Name	The username.
Type	Type of user.
Permissions	Type of user access.

Configuring Administrators

The following configuration options are available under *Administrators*:

- Changing the admin password on page 100
- Configuring Windows user accounts on page 100
- Configuring LDAP user accounts on page 100

Changing the admin password

By default, the *admin* user account has no password. You should add a password to increase security.

To change the admin password:

1. Go to *Administration* > *Administrators*.
2. Select the *admin* account.
3. Click *Change Password* from the toolbar. Change your password.
4. Click *Save*.

Configuring Windows user accounts

You can configure Windows users to have no access or administrator access to FortiClient EMS.

The Windows users list is derived from the server on which FortiClient EMS is installed. If you want to add more Windows users, you must add them to the server.

To configure Windows users:

1. Go to *Administration* > *Administrators*.
2. Click the *Add* button from the toolbar.
3. Perform one of the following actions:
   a. Select the specific domain access for the user. See Default user account and permissions on page 99.
   b. Configure the permissions. See Administrators reference on page 100.
4. Click *Save*.

Configuring LDAP user accounts

The list of LDAP users is derived from the server on which FortiClient EMS is installed. If you want to add more LDAP users, you must add them to the server.

To configure LDAP users:

1. Go to *Administration* > *Administrators*.
2. Click the *Add* from the toolbar.
3. Select the LDAP user.
4. Configure the options.
   a. Select the specific domain access for the user. See Default user account and permissions on page 99.
   b. Configure the permissions. See Administrators reference on page 100.
5. Click *Save*.

Administrators reference

This section contains descriptions of the fields used to configure *Administrators*.

Windows/LDAP users

Following is a description of the fields in *Administration* > *Administrators* > *Add*.

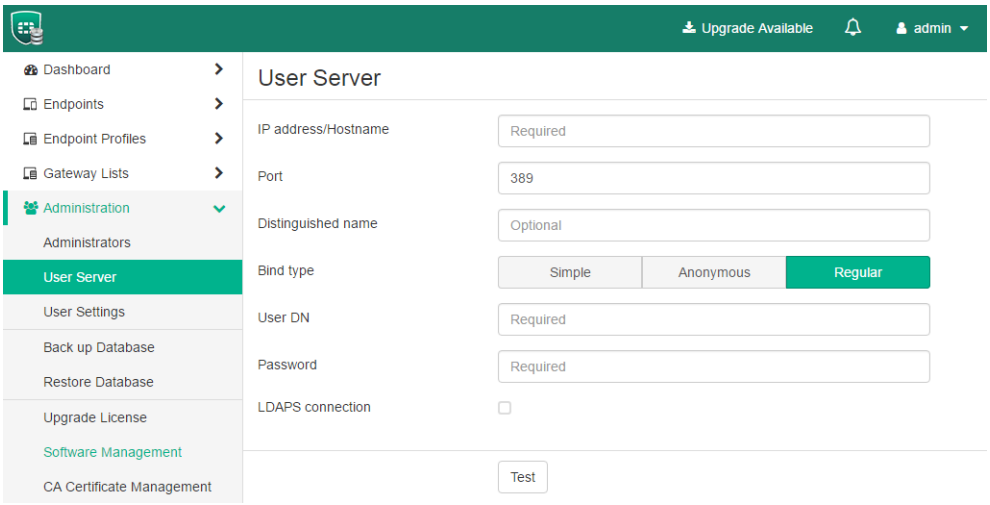
Option	Description
User	Select the Windows/LDAP user to configure permissions for FortiClient EMS.
Super Administrator permissions	Enable the super administrator feature to give the new Windows/LDAP user super administrator permissions.
Comment	Enter optional comments/information for the Windows/LDAP user.
Domain Access	Select or add access to a domain for the Windows/LDAP user and configure their permissions. If you choose one or more domains in the domain access field, you must select specific permissions.
General Permissions	Use the settings to configure permissions to FortiClient EMS for the selected Windows/LDAP user.
Create/Update/Delete LDAPs	Select to allow the Windows user to create, delete, and update LDAP records. Clear to disable this permission.
Create/Update/Delete custom groups	Select to allow the Windows user to create, update, and delete custom groups. Clear to disable this permission.
Create/Delete filters	Select to allow the Windows user to create and delete filters. Clear to disable this permission.
Endpoint Permissions	Use the following options to configure permissions for the selected Windows user.
Block/Unblock/Deregister/Quarantine/Unquarantine/Reregister endpoints	Select to allow the Windows user to block, unblock, disconnect, quarantine, unquarantine, and reconnect endpoints. Clear to disable this permission.
Run commands on endpoints	Select to allow the Windows user to run commands on endpoints. Clear to disable this permission.

Option	Description
Access Software Management	Select to allow the Windows user to access the *Administration* > *Software Management* options. Clear to disable this permission.
Access CA Certificate Management	Select to allow the Windows user to access the *Administration* > *CA Certificate Management* options. Clear to disable this permission.
Policy Permissions	
Assign/Unassign policies	Select to allow the Windows user to assign to endpoints and unassign profiles from endpoints and manage custom groups. Clear to disable this permission.
Create/Update/Delete policies	Select to allow the Windows user to create, delete, edit, and rename profiles. Clear to disable this permission.

Configuring User Server

To add a user server:

1. Go *Administration* > *User Server*. The settings display.



2. Configure the following options:

IP address/Hostname	Enter the server IP address or name.
Port	Enter the server port.

Distinguished name		Enter a distinguished name.
Bind type		Select either *Simple*, *Anonymous* or *Regular* for the bind type.
	User DN	Appears only when the *Regular* bind type is selected. Enter the username.
	Password	Appears only when the *Regular* bind type is selected. Enter the password.
	Show Password	Enable to show the password.
	LDAPS connection	Enable LDAPS connection.

3. Click *Test* to check the LDAP server settings.
4. Click *Save*.

Configuring User Settings

To configure User Settings:

1. Go to *Administration* > *User Settings*.
2. Set the following option:

Inactivity timeout	Specify how long to keep inactive users logged into FortiClient EMS. When the time expires, the user is automatically logged out of FortiClient EMS. Type 0 to keep inactive users logged into FortiClient EMS indefinitely.

3. Click *Save*.

Database management

You can back up and restore the FortiClient EMS database.

Backing up the database

To back up the database:

1. Go to *Administration* > *Back up Database*.
2. Set the following options:

Password	Type a password for backing up and restoring the database.
Confirm password	Retype the password to confirm it.

3. Click *Back up*.
   The database is backed up.

Restoring the database

To restore the database:

1. Go to *Administration* > *Restore Database*.
2. Click *Browse*.
3. Locate the database backup file, and click *Open*.
4. In the *Password* box, type the password used to back up the database.
5. Click *Restore*.
   When the database is restored, a message appears. The message instructs you to wait for the restored database to reload.
6. Wait for the restored database to be reloaded.

License upgrades or renewals

Contact Fortinet Support to upgrade or renew your FortiClient EMS license. After you have the license file, you can add it to FortiClient EMS.

To upgrade or renew the FortiClient EMS license:

1. Go to *Administration* > *Upgrade License*. The *Upgrade License* pane displays.
2. Click *Activate*, then click *Browse* and locate the license key file.
3. Click *Upload*.

Software Management

FortiGuard Distribution Network

FortiClient EMS automatically connects to FortiGuard Distribution Network (FDN) to provide access to FortiClient installers you can use with FortiClient EMS profiles. If a connection to FDN is not available, you must manually download FortiClient installers to use with FortiClient EMS. See Downloading FortiClient installers on page 104.

Downloading FortiClient installers

You can download FortiClient installers to use with FortiClient EMS from the following locations:

- Fortinet Customer Service & Support: https://support.fortinet.com
  Requires a support account with a valid support contract. Download the Microsoft Windows (32-bit/64-bit) or the Mac OS X installation file.
- FortiClient homepage: www.forticlient.com
  Download the FortiClient online installation file. The installer file performs a virus and malware scan of the target system prior to installing FortiClient.

Adding FortiClient installers

When you add a FortiClient installer to FortiClient EMS, you can specify what FortiClient features to include in the installer for the endpoint. You can include a feature in the installer, then disable the feature in the profile. Because the feature is included in the installer, you can update the profile later to enable the feature on the endpoint.

When you add a FortiClient installer to FortiClient EMS, an installer for the Windows operating system and an installer for the OS X operating system are added to FortiClient EMS.

After you add a FortiClient installer to FortiClient EMS, you cannot edit it. You can delete the installer from FortiClient EMS, and edit the installer outside of FortiClient EMS. You can then add the edited installer to FortiClient EMS.

To add FortiClient installers:

1. Go to *Administration* > *Software Management*.
2. Click *Add*.
3. On the *General* tab, set the following options:

Name	Type the FortiClient installer's name.
Notes	(Optional) Type any notes about the FortiClient installer.
Version	Select the FortiClient version to install. Click *Upload* to add a custom FortiClient installer.
Patch version	Select the specific FortiClient patch version to install.
Keep updated to the latest patch	Select to enable FortiClient to automatically update to the latest patch release when FortiClient is installed on an endpoint. This field is only available for the latest FortiClient version FortiClient EMS can access from FortiGuard. This option is not available if an older FortiClient version is selected.

4. Click *Next*. On the *Features* tab, set the following options:

Security Fabric Agent (Mandatory Feature)	Enabled by default and cannot be disabled. Installs FortiClient with Telemetry and Vulnerability Scanning enabled.
Secure Access Architecture Components	Enable to install FortiClient with SSL VPN and IPsec VPN enabled. Disable to omit SSL VPN and IPsec VPN support from the FortiClient installer.
Advanced Persistent Threat (APT) Components	Enable to install FortiClient with APT components enabled. Disable to omit APT components from the FortiClient installer. Includes FortiSandbox detection and quarantine features.

Additional Security Features	Enable to select one, two, or all of the following features: • AntiVirus • Web Filtering • Application Firewall • Single Sign-On mobility agent Disable to exclude the features from the FortiClient installer.
Enable automatic registration	Enable to configure FortiClient to automatically connect Telemetry to EMS or FortiGate after FortiClient is installed on the endpoint. Disable to turn off this feature and require endpoint users to manually connect Telemetry to EMS or FortiGate.
Enable desktop shortcut	Enable to configure the FortiClient installer to create a desktop shortcut on the endpoint.
Enable start menu shortcut	Enable to configure the FortiClient installer to create a Start menu shortcut on the endpoint.

5. Click *Next*. On the *Telemetry* tab, set the following options:

EMS	Click *EMS* to configure the FortiClient installer to connect Telemetry to EMS.
FortiGate	Click *FortiGate*, and select the name of the gateway IP list to use. The gateway IP list defines the IP address for FortiGate and includes the IP address for EMS. You must define a FortiClient Telemetry gateway IP list to select FortiGate. If you have not created a list, the *No Gateway IPs have been defined* dialog box is displayed, and you can click *OK* to create a list.

6. Click *Save*. The FortiClient installer is added to FortiClient EMS and displays on the *Software Management* pane.

If the *Sign software packages* option is enabled in *System Settings* > *Server*, Windows installers display as being from the publisher specified in the certificate file. See Configuring Server settings on page 111.

Uploading custom FortiClient installers

You can create a custom FortiClient installer and add it to FortiClient EMS. Alternately, if a connection to FDN is not available, you may need to manually download a FortiClient installer and add it to FortiClient EMS. See FortiGuard Distribution Network on page 104.

To add custom FortiClient installers to FortiClient EMS:

1. Download a FortiClient installer. See Downloading FortiClient installers on page 104.
2. Go to *Administration* > *Software Management*. The *Software Management* pane displays.
3. Click *Add*. The *Add Installer* dialog box displays.

4. On the *General* tab, set the following options:

Name	Type the FortiClient installer's name.
Notes	(Optional) Type any notes about the FortiClient installer.

5. In the *Version* list, select *Upload*. Uploading options display.
6. Set the following options:

Upload Windows Installers	Enable to upload FortiClient installers for the Windows operating system.
Windows 64-bit installer	Click the *Browse* button to locate and select a custom 64-bit installer for the Windows operating system.
Windows 32-bit installer	Click the *Browse* button to locate and select a custom 32-bit installer for the Windows operating system.
Upload Mac OS X Installers	Enable to upload a FortiClient installer for the OS X operating system.
Mac OS X installer	Click the *Browse* button to locate and select a custom installer for the OS X operating system.

7. On the *Telemetry* tab, set the following options:

EMS	Click *EMS* to configure the FortiClient installer to connect Telemetry to EMS.
FortiGate	Click *FortiGate*, and select the name of the gateway IP list to use. The gateway IP list defines the IP address for FortiGate and includes the IP address for EMS. You must define a FortiClient Telemetry gateway IP list to select FortiGate. If you have not created a list, the *No Gateway IPs have been defined* dialog box displays, and you can click *OK* to create a list.

8. Click *Save*. The installer is added to FortiClient EMS and displays on the *Software Management* pane.

If the *Sign software packages* option is enabled in *System Settings* > *Server*, Windows installers display as being from the publisher specified in the certificate file. See Configuring Server settings on page 111.

Viewing installers in Software Management

After you add FortiClient installers to FortiClient EMS, you can view them in *Software Management*.

To view FortiClient installers:

1. Go to *Administration* > *Software Management*.
   The *Software Management* pane displays available installers.

Available Installers	Lists the following information about each installer: • Operating system (Windows or OS X) • Version of FortiClient software • Name of the FortiClient installer • Location of the FortiClient installer FortiClient EMS. Endpoint users can access this location to download and install FortiClient on endpoints.
View Details	Lists the following information about the selected installer: • Name of the FortiClient installer • Operating system (Windows or OS X) • Version of FortiClient software • Enabled features • Managed by FortiGate or FortiClient EMS • Telemetry connection IP address • Auto update enabled/disabled • Desktop shortcut enabled/disabled • Start menu shortcut enabled/disabled
Delete	Click to delete the FortiClient installer.
Add	Click to add a FortiClient installer.
Refresh	Click to refresh the FortiClient installer list.

Deleting FortiClient installers

To delete FortiClient installers:

1. Go to *Administration* > *Software Management*. The *Software Management* pane displays.
2. Click the desired installer, then click the *Delete* button.
   A confirmation dialog box displays.
3. Click *Yes*.
   The FortiClient installer is deleted from FortiClient EMS.

CA Certificate Management

You can upload or import CA certificates into FortiClient EMS.

Uploading certificates

You can locally upload a CA certificate.

To upload a certificate:

1. Go to *Administration* > *CA Certificate Management*.
2. Select *Upload*.
3. In the *Upload Local Certificate* window, click *Browse* and locate the certificate.
4. Click *Upload*.

Importing certificates

To import certificates:

1. Go to *Administration* > *CA Certificate Management*.
2. Select *Import*.
3. In the *Import Certificates from FortiGate* window, enter the following information:

IP address/Hostname	Enter the server IP/hostname in the following format: `<ip address> : <port>`.
VDOM	Enter the VDOM.
Username	Enter the username.
Password	Enter the password.

4. Click *Import* to import the certificate.

Logs

You can view the log messages generated by FortiClient EMS and download raw logs.

Viewing logs

To view log messages:

1. Go to *Administration* > *View and Download Logs*.
2. Click the *Filter* icon in each column heading to apply filters.
3. Click *Clear Filters* to remove the filters.

Downloading logs

You can download the logs generated by FortiClient EMS.

To download logs:

1. Go to *Administration* > *View and Download Logs*.
2. Click *Download*.
   A zip of the raw logs is downloaded to your computer.

System Settings

This section describes FortiClient EMS settings.

Configuring Server settings

FortiClient EMS installs with a default IP address and port configured. You can change the IP address and port and configure other server settings for FortiClient EMS.

To configure Server settings:

1. Go to *System Settings* > *Server*.
2. Configure the following options:

Hostname	Displays the FortiClient EMS server's host name.
Listen on IP	Displays the IP addresses for the FortiClient EMS server. FortiClient connects to FortiClient EMS on the specified IP address.
Listen on port	Displays the default port for the FortiClient EMS server. You can change the port by typing a new port number. FortiClient connects using the specified port number.
Upload port	Displays the default port used for FortiClient to upload large amounts of data (100+ KB of data per connection) to FortiClient EMS. You can change the port by typing a new port number.
Use FQDN	Turn on to specify a fully qualified domain name (FQDN) for the FortiClient EMS server.
FQDN	Displayed when *Use FQDN* is turned on. Type the FQDN for the FortiClient EMS server. FortiClient can connect using the specified IP address in the *Listen on IP Addresses* option or the specified FQDN.

DHCP onnet/offnet

Enable to monitor endpoints within the company network (onnet).

Endpoints connected to FortiClient EMS from outside the company network (offnet).

There are two settings in EMS that affect the FortiClient onnet/offnet status:

1. DHCP onnet/offnet setting in EMS
2. Subnet setting in EMS

Onnet/Offnet Matrix:

DHCP Onnet/Offnet Setting	Subnet Setting	DHCP 224 Option	Result
off	no	N/A	onnet
off or on	yes, match	N/A	onnet
off	yes, not match	N/A	offnet
on	yes or no	option configured	onnet

Notes:

Subnet values:

no: subnet setting in EMS is disabled

yes: subnet setting in EMS is configured

match: client has an IP in the configured EMS subnet

not match: client has IP not in the configured EMS subnet

Examples on how EMS determines the status for the endpoint:

- The endpoint has a status of offline when the endpoint cannot connect FortiClient Telemetry to EMS, and the endpoint is outside one of the onnet networks.
- The endpoint has a status of offline but onnet when the endpoint cannot connect FortiClient Telemetry to EMS. However, the endpoint is inside one of the onnet networks.

Option 224 can have any serial number of a Fortinet device. EMS assumes FortiClient is behind a FortiGate, and it is onnet with that FortiGate.

Remote HTTPS access

Specify settings for remote administration access to FortiClient EMS.

Turn remote HTTPS access to FortiClient EMS console on and off. When enabled, type a host name in the *Custom Host Name* box to let administrators use a browser and HTTPS to log into the FortiClient EMS console. When disabled, administrators can only log into FortiClient EMS console on the server.

Pre-defined hostname

Available when *Remote Administration HTTPS Access* is turned on. Displays the pre-defined host name. The name cannot be changed.

	Custom hostname	Available when *Remote Administration HTTPS Access* is turned on. Displays the pre-defined host name of the server on which FortiClient EMS is installed. You can customize the host name. When you change the host name, the web server restarts.
	Redirect HTTP request to HTTPS	Available when *Remote Administration HTTPS Access* is turned on. If this option is enabled, if you attempt to remotely access EMS at *http://<server_name>*, this is automatically redirected to *https://<server_name>*.
FortiClient download URL		FortiClient installers created in FortiClient EMS will be made available for download at the URL.
	Open port 10443 in Windows Firewall	Turn on to open port 10443, and turn off to close port 10443. Port 10443 is used to download FortiClient.
SSL certificate		Displays the SSL certificate currently imported. If you have not imported an SSL certificate, a *No SSL certificate imported* message displays.
New SSL Certificate File		Upload a new SSL certificate.
New SSL Private Key		Upload a new SSL private key.
Sign software packages		Enable this option to have Windows FortiClient software installers created by or uploaded to EMS digitally signed with a code signing certificate.
	Timestamp server	Enter the server address to timestamp software installers with.
	Certificate	Upload the desired code signing certificate. This must be a .pfx file. After a certificate has been uploaded, its expiry date is also displayed.
	Password	Enter the certificate password. This is required for EMS to sign the software installers with the certificate.

3. Click *Save*.

Configuring Logs settings

You can specify what level of log messages to capture in the logs for FortiClient EMS. You can also specify when to automatically delete logs and alerts.

To configure Logs settings:

1. Go to *System Settings* > *Logs*.
2. Configure the following options:

Log level	Select the level of messages to include in FortiClient EMS logs. For example, if you select *Info*, all log messages from *Info* to *Emergency* are added to the FortiClient EMS logs.
Clear logs every	Type the number of days that you want to store logs. For example, if you type 30, logs will be stored for 30 days. Any logs older than 30 days are automatically deleted.
Clear alerts every	Type the number of days that you want to keep alerts. For example, if you type 30, alerts will be kept for 30 days. Any alerts older than 30 days are automatically deleted.
Clear now	Click to immediately delete all FortiClient EMS logs or alerts.

3. Click *Save*.

Configuring FortiGuard settings

To configure FortiGuard settings:

1. Go to *System Settings* > *FortiGuard*.
2. Configure the following options:

Use FortiManager for client software/signature updates	Turn on to use FortiManager for updating FortiClient software or signatures. You must specify the IP address or host name for FortiManager as well as the port number.
IP address/Hostname	Enter the IP address/host name.
Port	Configure the port number.
Failover port	Configure the failover port.
Timeout	Configure the timeout interval (in seconds).
Failover	Enable failover to FDN when FortiManager is not available.
Use proxy to access update server	Turn on to specify a proxy for updates to FortiClient software.
IP address/Hostname	Enter the IP address/host name.
Port	Configure the port.
Username	Configure the username. This is optional.
Password	Configure the password.

3. Click *Save*.

Configuring Endpoints settings

To configure Endpoints settings:

1. Go to *System Settings* > *Endpoints*.
2. Configure the following options:

FortiClient telemetry connection key	Add the FortiClient Telemetry connection key for FortiClient EMS. FortiClient must provide this key during connection.
Keep alive interval	Each connected FortiClient sends a short keep-alive message to FortiClient EMS at the specified interval.
Full keep alive interval	Each connected FortiClient sends a full keep-alive message to FortiClient EMS at the specified interval.
License timeout	Each connected FortiClient consumes a license seat. If an endpoint disconnects from EMS, the license seat is retained in anticipation that the endpoint will reconnect. If the endpoint does not reconnect within the given timeout, its connection record is removed from EMS. If the endpoint is removed, switched off, or becomes offline, and does not reconnect to EMS within the given timeout, the endpoint is removed from EMS even if it is still connected to EMS.
Automatically upload avatars	When enabled, FortiClient uploads user avatars to all FortiGate units, FortiAnalyzer units, and EMS servers it is connected to.

3. Click *Save*.

Configuring the login banner

When you enable the login banner, a message appears prior to a user logging into EMS.

To enable and configure a login banner:

1. Go to *System Settings* > *Login Banner*.
2. Click *Enable login banner*.
3. In the *Message* box, type your message. The *Preview* section displays a preview of the message.
4. Click *Save*.

Configuring EMS Alerts

You can set up an SMTP server to enable alerts for EMS or endpoint events. When an alert is triggered, an email notification is sent.

To configure email alerts and an SMTP server:

1. Go to *System Settings* > *EMS Alerts*.
2. Set the following options to send an email when the following events happen:

New EMS version is available for deployment	New EMS version is available.
Remind me everyday for 2 weeks	Enable to remind you when new EMS versions are available everyday for two weeks.
New FortiClient version is available for deployment	New FortiClient version available for deployment.
Remind me everyday for 2 weeks	Enable to remind you when new FortiClient versions are available everyday for two weeks.
EMS license is expired or about to expire	Expiring or expired EMS license.
EMS fails to sync with LDAP domains	EMS does not sync with LDAP domains.
Less than 10% of client licenses are left	Enable to be notified when there are less than 10% of client licenses left.
Client licenses have run out	Enable to be notified when you run out of client licenses.

3. Go to *System Settings* > *Endpoint Alerts* and set the following options:

Send an email every	Configure the time interval email alerts are sent. Options include: • 1 minute • 5 minutes • 10 minutes • 15 minutes • 30 minutes • 1 hour • 2 hours • 6 hours • 12 hours • 1 day
Malware is detected	Malware detected.
Repeated malware is detected	Same malware is detected on the same machine in the last 24 hours.
Multiple malwares are detected	Different malware is detected on the same machine in the last 24 hours.
Malware outbreak is detected	Same malware is detected on different endpoints in the last 24 hours.

Zero-day malware is detected by FortiSandbox	Previously unknown computer virus or other malware for which specific antivirus software signatures are not yet available.
C&C attack communication channel is detected	Command and control attack communication channel is detected.
Critical vulnerability is detected	Critical vulnerability detected,
Endpoint FortiClient Telemetry is manually disconnected by user	FortiClient Telemetry endpoint is manually disconnected by user.
Endpoint signature database is out-of-date	Out-of-date endpoint signature is detected.
Endpoint software is out-of-date	Out-of-date endpoint software is detected.
Endpoint is not compliant	Endpoint does not adhere to compliance rules.

4. Click *Save*.
   If you have not already set up an SMTP server, the GUI automatically prompts you to configure SMTP server settings. See Configuring SMTP Server settings on page 117.

Configuring SMTP Server settings

You can set up an SMTP server to enable alerts for EMS events. When an alert is triggered, an email notification is sent.

To configure SMTP Server settings:

1. Go to *System Settings* > *SMTP Server*.
2. Set the following options:

Server		Enter the SMTP server.
Port		Enter the port number.
Security		Select *None*, *STARTTLS*, or *SMTPS* for the security type, or select the *Auto Detect* button to automatically select the security type. If *STARTTLS* or *SMTPS* is selected, the *Username* and *Password* boxes become available.
	Username	Enter the username.
	Password	Enter the password.
From		Enter the email address to send the alerts from.
Reply-To		Enter the email address to send the replies to.
Subject		The sent e-mail alert's subject.

Recipients	Enter email address(es) to send alerts to. Click the + button to add more email addresses.
Test Subject	Test email's subject.
Test Message	Test email's message.
Test Recipient	Email address to send the test email to.
Send Test Email	Click the button to test the configured email settings.

3. Click *Save*.

Viewing Alerts

You can view alerts FortiClient EMS generates. Examples of events that generate an alert include:

- New version of FortiClient is available
- FortiClient deployment failed
- Failure to check for signature updates
- Error encountered when downloading AD server entries
- Error encountered when scanning for local computers

A red label is associated with the *Alert* icon when new notifications are available or received. It is cleared when you view the alert.

To view alerts:

1. Click the *Alert* icon (a bell) in the toolbar.
2. Click the *Filter* icon in each column heading to apply filters.
3. Click *Clear Filters* to remove the filters.

Creating a Support Package

You can create a support package to provide to the Fortinet technical support team for troubleshooting. Creating a support package backs up your database, but clears all sensitive username and password fields.

To create a support package:

1. Go to *Help* > *Create Support Package*. The *Create Support Package* dialog box displays.
2. In the *Password* box, type your administrative password.
3. In the *Confirm Password* box, type your password again.
4. Click *Create Support Package*.